Information Technology Change and the Effects on User Behavior and Cyber Security

Emergent Research Forum

Introduction

New technology implementation can have a critical effect on the user behavior and can impact the security posture of an IS organization's network systems. Changes brought on by new technology can enable better user performance, however, some users may find it difficult to adjust to using new software applications and may elect to circumvent the system security features in order to get their job done. This type of user behavior may be viewed as non-intentional malicious behavior because the user elected to by-pass the security policy.

Purpose

The purpose of this study is to examine the security related changes that organizations need to consider for maintaining a good security posture in respect to users on their networks when an information technology change occurs within the organization. In particular, this study will focus on how user behavior is affected as they learn how to use a new application or process that is introduced by the new change of information technology in network systems.

In this study we will examine key factors that influence the negative user behavior after an IT change and implementation along with any security modifications required for maintaining a good network security posture within the organization. In the past, negative user behavior has been under-researched. In order to better understand the influence of negative user behavior factors a theoretical model will be proposed in order to analyze these effects after a new IT change is made by an IS organization.

This study is important because of the recent insider threat incidents that have occurred against U.S. government systems and commercial credit card accounts. In addition, as IS organizations implement the use of new technology within their networks new cyber threats may also be made available to negative users on their networks.

With the recent increase in network security threats from within an IS organization there is a strong need to study these factors that influence negative user behavior. There is a gap in the amount of research that has been accomplished in assessing negative user behavior and the factors that influence this type of behavior (Warkentin et al, 2012).

The primary research question for this study then is: "Does new change in IT influence an IS organization's network user behavior toward negative intent?"

The second research question that this study will also consider is: "How can IS organizations counter malicious user behavior on their network systems after implementation of new technology upgrade?"

Literature Review

Two user behavior related studies form the basis for this paper, Leonard et al. (2005) and Blanke (2008), and will be used to develop the theoretical framework and a conceptual model for a better understanding of user behavior on IS network systems whenever an IT change is implemented. IT change in the organization can be considered a change in the professional environment of an individual and may have an impact on their network user behavior.

Security information & event management (SIEM) technology can be used to keep track of user logged access as well as compliance of security training requirements (Miller et al., 2011). The correlation capabilities of commercially available SIEM technology can be expanded to include tracking of users meeting training requirements and if the user is non-complaint the SIEM controls can deny them access to system information.

This type of access control can be viewed as either a reward or fear of punishment and loss of trust that is in line with the study by (Alder et al., 2006). The monitoring of training completion of the user by SIEM technology may also be viewed in a similar manner as the electronic performance measure (EPM) described in the study by (Samaranayake et al., 2011). The combination of user behavior monitoring of their training along with meeting system security policy and information assurance compliance and security controls is an extension of the research done by D'Arcy & Hovav (2009).

The study by Leonard and Cronan (Leonard et al., 2005) examined ethical behavior concerning Information Systems and computer use. An earlier study by Kreie and Cronan (Kreie et al., 1999) provides initial findings of a similar effort concerning attitudes and ethical behavior. Haines & Leonard (2005) build on the environmental influences (societal, belief system, personal, professional, legal, and business) that Kreie used in the 1999 article. One additional consideration that Leonard looks into in this study is the role of gender in attitude differences.

The recommendations by Leonard et al., (2005) are in-line with the current study that looks for the effects on employee behavior as not only ethical employee attitude and behavior but also to include new IT change as it is being developed and integrated to improve employee network performance.

Blanke (2008) presents a study of the potential computer abuse intent by employees based on computer security policy awareness, computer self-efficacy, and attitude toward computer abuse. Attitude is defined as an individual's degree of favorable or unfavorable evaluation of a behavior (Blanke, 2008).

The type of computer abuse that Blanke (2008) researches includes computer misuse by employees for personal use, loss of productivity while employees conduct personal business at work, and internet surfing during work hours. An employee who misuses an organization's network system for personal use may incur a loss of productivity if this activity occurs during working hours and is against the organization's security policy (Blanke, 2008).

Blanke (2008) proposes a model to help measure the effects of the three factors mentioned above in order to identify the most significant of the three towards computer abuse intent. The model that is utilized by Blanke is not a new model, but one that has been used by others, however, the intent is to measure and account for the effects.

The method employed by Blanke (2008) was a predictive study that attempted to assess and predict the employees' computer abuse intent (CAI) in business environments based on the contribution of attitude (ATT), computer security policy awareness (CSPA), and computer self-efficacy (CSE). The dependent variable is CAI and the independent variables in the study are ATT, CSPA and CSE.

The results of this study (Blanke, 2008) showed that CSPA was not a significant factor or major influencer of CAI. CSE was a significant factor in some cases. Overall ATT was the most significant factor and influencer on CAI. Blanke (2008) admits that her study and results are limited and cannot be generalized primarily due to the sample population of college students and the method used to administer the survey via a website and the collection of the data. This study may be helpful in this current research project in that it could help identify a potential model to use to measure the counter effects of employee behavior as they are being monitored while on the job in real-time.

In this study a literature review of related user behavior studies is performed in order to help identify and list the most common and key predictors that may influence the employee's attitude toward computer

negative intent. The results of predictors for both areas of human behavior and IT security are listed in Table 1 below:

Articles	Independent Variables Human Behavior	Independent Variables IT Security
Reznik et al, 2012	security habits	passwords, anti-virus, patching
Warkentin, et al, 2012	individual behaviors, attitudes, intentions	security policy, SETA, Information Assurance
Leonard et al, 2004	personal, social, environmental	
Cronan et al, 2005	attitude, ethical behavior perceived importance	
Alder et al, 2006	justification, advance notice, perceived organizational support	internet monitoring
Posey et al, 2011	behavioral information security, causal reasoning attributed trust	management style, organizational structure
Greitzer & Hohimer, 2011	triggers, human behaviors	forensics,
Leach, 2003	user security behaviors, personal values, security common sense	leadership & management security support
Stanton et al, 2004	user behavior, naïve mistakes, intentional destruction	computer security, organizational management surveys
Goodhue & Straub, 1991	system misuse, awareness knowledge of systems	IS environment, organizational actions
Willison & Warkentin, 2013	computer abuse, employee computer crime, motivation, disgruntlement, insider	Information Systems security, organizational justice
Mathieson, 1991	attitude, subjective norms, perceived behavioral control	
Chen et al, 2012	punishment, reward, certainty of control	information security policy, compliance theory
Posey et al, 2013	protection-motivated behaviors, insider, behavioral information security	Systematic s
D'Arcy & Hovav, 2009	user awareness, self-efficacy, virtual status	SETA, security policy, computer monitoring

Table 1. Articles' Constructs List

For this study the decision was made to focus the human behavior predictors for the proposed developmental model to include: 1) personal values; 2) moral obligation; and 3) belief system. These three human behavior predictors were selected because they deal with the user behavior at the individual level. The IT security related predictors for the proposed developmental model include: 1) security policy; 2) SETA; and 3) information assurance. These three IT security related predictors were selected because they best represent the organization's security environment.

Methodology

The methodology for this study will include both surveys and a case study in order to collect both data from the behavior aspect as well as from the number of security incidents over a period of time after an organization's IT change. The survey interviews will include samples from everyone who has access to network security systems within an IS organization including security managers, employees, and network service and maintenance personnel. The interviews with IS organization security managers will provide information concerning the trends in cyber security and user behavior that may have occurred with the system changes using new technology. The employee surveys will provide data for analysis of their behavior and potential misuse of network systems that have been changed or upgraded. The literature review will assist in identifying any trends or patterns of user behavior from past studies.

In related security compliance studies data was collected in surveys from both managers and employees (Alder et al, 2006). For this study the proposed method is to conduct a case study that includes interviews with both managers and employees as well as collecting security related data from an IS organization in order to determine the number of security incidents and change in security posture of the organization at a particular point in time. For example, if security assessment measures (SAM) are conducted before an IT change then a security posture baseline can be established to help assess the improvement/degradation related to the IT change based on the number of security related incidents. The security incidents may not have to be related entirely to network use and could include phone use or other electronic means of communication misuse (McNall & Roch, 2009). This type of user monitoring could lead to a decline in morale and have a negative effect on employee performance (Alder et al., 2006).

In a recent study (Chivers et al., 2013) each user on a network is treated as node in the network and its associated performance characteristics are compared to a normal level of activity in order to help identify behavioral patterns and to distinguish abnormal network activity (Miller et al., 2011).

A study by Willison & Warkentin (2013) is based on a new expanded security action cycle framework that also looks for abnormal behavior by the user before an attack occurs. The General Deterrence Theory, according to D'Arcy & Hovav (2009) can help convince some users that the chances are high of getting caught and punished for computer system misuse. All of these methods have one thing in common and that is to deter any network attack from within as early in the cycle as possible.

Proposed Model

The proposed theoretical model in Figure 1. will be based primarily on Information Technology (IT) ethical behavior model presented by Leonard et al. (2004). The model proposed by Leonard et al. (2004) includes constructs such as attitude, perceived importance, subjective norms, situational factors, and individual characteristics.

In addition, the proposed theoretical model for this study will also consider two major and well known theories: 1) Theory of Planned Behavior (Ajzen 1991); and 2) the Technology Acceptance Model (Mathieson, 1991) (Davis, 1989). We propose that the more ethical an individual has as personal values, moral obligation, and belief system the relationship with attitude will be positive.

Also, we propose that the better the security policy, SETA, and IA in place within an organization the relationship with attitude will also be positive. In addition, the relationship between attitude and computer abuse intention in our theoretical model will be negative. The more ethical that one behaves at work the less their computer abuse intention will be.

This logic is similar in reasoning as has been found in past studies concerning the Theory of Planned Behavior and the Technology Acceptance Model.

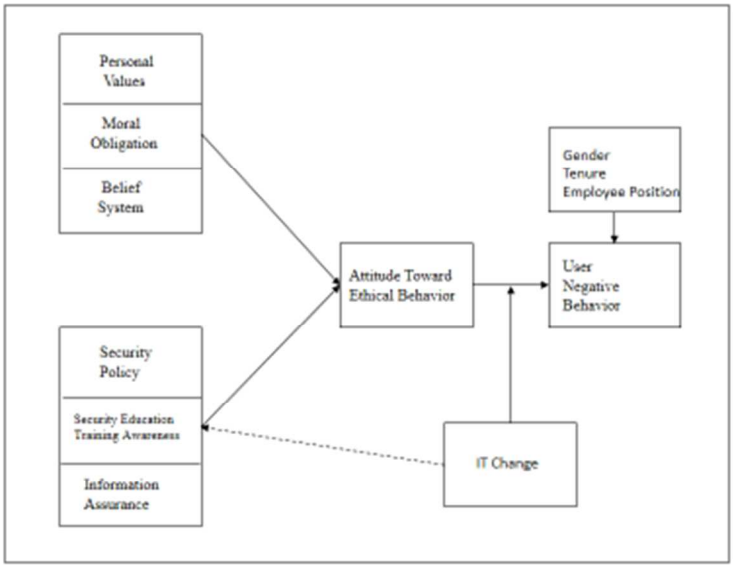

Figure 1. Proposed Theoretical Model

The proposed model will have an additional factor (IT Change) that will be assessed for moderation effects on user intent for negative behavior. The IT Change can also be viewed as the "trigger" mechanism that sets off the change in the organization's security environment.

Expected Results/Contribution

The expected results of this study are presented in the Figure 2 below.

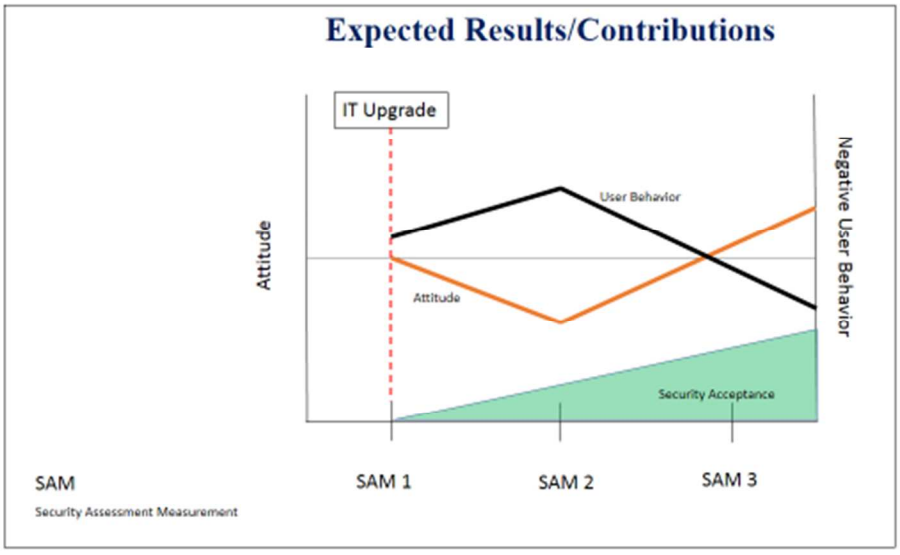

Figure 2. Expected Results and Contributions

On the left vertical axis is a notional scale of the user attitude and on the left vertical axis is a notional scale of negative user behavior. On the horizontal axis is a notional timeline that begins with attitude and user behavior at some "normal" level.

Soon after the IT Change occurs (SAM 1) we should logically observe a decrease in user attitude and an increase in negative user behavior. At SAM 2, there is a change in the direction for both attitude and for negative user behavior. In addition, there is a slight increase in user security acceptance as system users get accustomed to the new IT change and the related new security features implemented.

At some point between SAM 2 and SAM 3 there will be a crossing-point between the increasing slope of user attitude and the decreasing slope of negative user behavior before they settle at a new "normal" operational level.

The user security acceptance level will also max out after the crossing-point between the user attitude and negative user behavior slopes.

In order to maintain this state of operations an organization will need to constantly monitor user behavior and assess where security changes need to be made according to future security assessment measurements.

The results/findings from this study will assist security managers to better understand changes in user behavior as new technology upgrades are introduced into the organization's network systems. In addition, by identifying the effects of new technology upgrades on computer user behavior and possible malicious intent, new counter-measures can be employed in order to maintain a proper security posture within the organization.

An example of the survey material is show in Appendix A. that will be part of the first pilot test in order to help provide support for the research model. After the measures have been evaluated and refined a larger set of data collection will be utilized for analysis.

Appendix A.

Scenario and Survey Item Sample:

Scenario 1

Joe is finishing up his work for the day and notices that a fellow co-worker, Tom, has left his computer on. Joe knows that Tom is gone for the day because Tom stopped by his desk to say good night. There is no one else in the office and it is just about time for the contractor cleaning crew to come in and clean the area. Joe does not turn off Tom's computer and leaves for the night.

PART A: What was the ***degree of influence*** for each factor in your assessment of why Joe did not turn off Tom's computer?

Degree of influence:	Great	Much	Moderate	Little	None
Belief system (Religious values and beliefs developed in one's spiritual or religious environment.)					
Personal values (Your personal values and experience.)					

PART B: How morally obligated would you feel to take corrective action in this case?

no obligation |___|___|___|___|___| ***strong obligation***

PART C:	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
P5. My organization has specific guidelines that govern what employees are allowed to do with their computers.					
SETA1. My organization provides training to help employees improve their awareness of computer and information security issues.					
IA4. I believe that my organization reviews logs of employees' computing activities on a regular basis.					
ATT5. To me, committing computer abuse is unacceptable.					

References

Alder, Stoney G., Noel, Terry W., & Ambrose, Maureen L. 2006. "Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust," *Information & Management*, (43), pp. 894-903.

Ajzen, I. Pratkanis, A.R., Breckler, S.J. and Greenwald, A.G. (Eds) 1998. *Attitude, Structure and Function,* Hillsdale, NJ: Lawrence Erlbaum Associates.

Ajzen, Icek 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, (50), pp. 179-211.

Blanke, Sandra J. 2008. "A study of the contributions of attitude, computer security policy awareness, and computer self-efficacy to the employee's computer abuse intention in business environment," *Nova Southeastern University*.

Chen, Yan, Ramamurthy, K. (RAM), & Wen, Kuang-Wei. 2013. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?" *Journal of Management Information Systems* (29), pp. 157-188.

Cronan, Timothy Paul, Leonard, Lori N. K., & Kreie, Jennifer 2005. "An Empirical Validation of Perceived Importance and Behavior Intention in IT Ethics," *Journal of Business Ethics* (56), pp. 231-238.

D'Arcy, John, & Hovav, Anat 2009. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics* (89), pp. 59-71.

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

Ferrell, O.C. & Gresham, L.G. 1985. "A contingency framework for understanding ethical decision making in marketing," *Journal of Marketing* (49), pp. 87-96.

Goodhue, Dale L., & Straub, Detmar W. 1991. "Security Concerns of System Users A Study of Perceptions of the Adequacy of Security," *Information & Management* (20), pp. 13-27.

Haines, Russell, & Leonard, Lori N.K. 2007. "Situational influences on ethical decision-making in an IT context," *Information & Management* (44), pp. 313-320.

Leach, Dr. John 2003."Improving User Security Behaviour," *Computer & Security* (22:8), pp.685-692.

Leonard, Lori N.K., & Cronan, Timothy Paul 2005. "Attitude toward ethical behavior in computer use: a shifting model," *Industrial Management & Data Systems* (105:9).

Leonard, Lori N.K., & Cronan, Timothy Paul, & Kreie, Jennifer 2004. "What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics?" *Information & Management* (42), pp. 143-158.

Mathieson, Kieran 1991."Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior," *Information Systems Research* (2:3), pp. 173-191.

Miller, David R., Harris, Shon, Harper, Allen A., Van Dyke, Stephen, & Blask, Chris 2011. *Security Information and Even Management (SIEM) Implementation*, New York, NY: *McGraw Hill*.

Posey, Clay, Bennett, Rebecca J., & Roberts, Tom L. 2011. "Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes," *Computers & Security* (30), pp. 486-497.

Posey, Clay, Roberts, Tom L., Lowry, Paul Benjamin, Bennett, Rebecca J., & Courtney, James F. 2013. *MIS Quarterly* (37:4), pp. 1189-1210.

Samaranayake, Viraj, & Gamage, Chandana 2011. "Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka," *Telematics and Informatics* (29), pp. 233-244.

Stanton, Jeffrey M., Stam, Kathryn R., Mastrangelo, Paul, & Jolton, Jeffrey 2004. "Analysis of end user security behaviors," *Computers & Security* (24), pp. 124-133.

Schwartz, S.H. & Tessler, R.C. 1972. "A test of model for reducing measured attitude-behavior discrepancies," *Journal of Personality and Social Psychology* (24), pp. 225-236.

Reznik, Leon, Christian, Andrew, Patel, Ankit, Treich, Brian, & Alromaih, Mohammed 2012. "The Current State of Ordinary User Security," *Annual Symposium on Information Assurance & Secure Knowledge Management*, Proceedings, pp. 62-67.

Warkentin, Merrill, Straub, Detmar, & Malimage, Kalana. Featured Talk: Measuring Secure Behavior: A Research Commentary. *Annual Symposium on Information Assurance & Secure Knowledge Management*, Proceedings, (2012), 1-8.

Willison, Robert & Warkentin, Merrill. Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly,* 37(1), (2013), 1-20.