Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance

Tonia SanNicolas-Rocca
San Jose State University
tonia.sannicolas-rocca@sjsu.edu

Benjamin Schooley
University of South Carolina
ben.schooley@sc.edu

Janine L. Spears
DePaul University
jspears@cdm.depaul.edu

Abstract

Institutions of higher education capture, store and disseminate information that is protected by state and federal regulations. As a result, IS security policies are developed and implemented to ensure end user compliance. This case study investigates end user knowledge of their university's IS security policy and proposes a new approach to improve end user compliance. The results of this study suggest that users may be contributors to the transfer of IS security policies when provided with an opportunity to participate in the development of an IS security awareness and training program.

1. Introduction

Institutions of higher education collect, store and disseminate information that is protected by state and federal regulations including the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and Protections of Pupil Rights Amendment (PPRA). In response, higher education organizations are tasked with guiding their institutions in the quest to safeguard data, information systems, and networks; protect the privacy of the higher education community; and ensure that information security is an integral part of campus activities and business processes [1].

The development and implementation of an information systems (IS) security policy is a mechanism used by institutions of higher education to guide business processes, organizational tasks and activities, and to ensure compliance to state and federal laws and regulations. It has been reported extensively that employees, also known as insiders, do not comply with IS security policies [2; 3; 4; 5; 6; 7]. If users do not comply, institutions of higher education could be at serious risk of regulatory liabilities and lawsuits [4; 8; 9].

IS security, however, continues to be a managerial concern, and has been identified as one of the top challenges facing institutions of higher education [1]. According to [10] approximately 200 institutions of higher education reported data breaches between 2010 and April, 2013. Of these incidents, approximately 80 were due to end user activity, including the unintended disclosure of and/or an insider's explicit intent to share sensitive information.

In other reports, users have directly or indirectly caused over half of all reported security breaches [11]. Insider threat continues to be a significant challenge, captures a great deal of public attention [7] [12] and methods to improve compliance are needed.

To improve compliance, organizations have relied on IS security education, training and awareness (SETA) programs. Although it is widely accepted that these programs are important for maintaining the effectiveness of information security and privacy techniques and procedures for user compliance [9; 13], it is also important to recognize that many of these programs have been considered useless [14] or have been found ineffective [15].

The success of SETA programs depends on the ability of the training facilitator to engage trainees [16]. When the instructor is able to effectively communicate the applicability and practical purpose of the material to be mastered, as distinguished from abstract or conceptual learning, the learning retention rates and the subsequent transference of the new knowledge or skill to the trainees is enhanced [17]. For IS security programs aimed at user compliance, this essentially means that the training method can affect the transference of knowledge to trainees, which can therefore influence the effectiveness of IS security training and awareness programs.

The theory of knowledge transfer has been discussed in the IS literature [18; 19]. Several factors have been identified as having an influence on knowledge transfer in the implementation of information systems [20]. These include absorptive

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.427

IEEE computer society

capacity, motivation, and communication [18; 20]. However, empirical results regarding the effects of knowledge transfer in IS security training or awareness for user compliance have not been reported. Furthermore, addressing knowledge transfer in IS security training and awareness for user compliance where the user is not only trained, but actively participates in the development of an IS security program has not been reported. This study addresses these gaps by focusing on user training and participation in the development of an IS security program within higher education to improve end user compliance.

The remainder of this paper proceeds as follows. First, a review of knowledge transfer, and user participation in information systems development is covered. We then describe the research location and method used. This is followed by a discussion of the findings, and implications for practice and research.

2. Literature Review

2.1. Knowledge Transfer

Knowledge is taken to be transferred when learning takes place and when the recipient understands the intricacies and implications associated with that knowledge so that he or she can apply it [20]. For example, trainers may transfer knowledge about their organization's IS security policy to users who learn and apply this knowledge. The knowledge is applied when evidenced by users communicating, teaching, and/or complying with IS security policies and regulations.

Knowledge transfer is influenced by three factors [20; 21; 18]: (1) Absorptive Capacity, (2) Motivation [22], and (3) Communication.

Absorptive Capacity

Absorptive capacity has been found to be positively related to knowledge transfer [22]. It is the ability of a recipient to recognize the importance and value of externally sourced knowledge, assimilate it, and apply it [23]. Absorptive capacity is largely a function of the recipient's existing knowledge prior to the transfer. Activating users' prior knowledge enhances their ability to process new information [22; 24]. IS researchers have found that a key problem regarding users' roles in information security work is their lack of prior or existing knowledge regarding information security and the implementation of security-related procedures [3; 15].

Motivation

Knowledge transfer can be influenced by the motivational disposition of the receiving unit (i.e., their willingness to acquire knowledge from the source) [18]. A key challenge regarding the role of employees in information security work is a lack of motivation regarding information security and related practice [15]. For example, it was reported that employees fail to use the information shared with them regarding IS security policies for the protection of sensitive information because they don't participate in the development of IS security policies and procedures [15] or see how information security integrates with their normal work activities. Employees also report that they do not see management taking an active role in promoting or complying with information security policies and instructions [22]. These factors have influenced the level of motivation, or lack thereof, for knowledge transfer to occur. Such motivation has been positively related to user compliance [22].

Communication

Many of the SETA programs implemented by organizations involve knowledge transfer channels that are considered ineffective and lead to an inability of the recipient to process the knowledge required to comply with IS security policies [15]. These programs include the use of mass-media awareness campaigns (e.g., leaflets, booklets, films, posters, direct mail) [15], IT-based training systems (e.g., interactive video training, web-based training, computer-based training, and video games) [16; 25], and instructor-led teaching with one-way interaction [26; 27].

[15] reported that a face-to-face, two-way communication training program can be the most effective tool to influence user behavior and awareness toward IS security practices as it (1) aims to create an understanding among users on why it is important for each user to pay attention to information security, which should make acceptance of technological, individual and administrative security measures smoother; (2) allows users to problem solve and ask questions; (3) allows users to reflect on their own situation such as asking "is there anything I could do differently to improve information security and why should I act differently in a world of conflicting demands?"; (4) allows users to meet IS security professionals face-to-face, thus making information security management more visible; and (5) creates motivation and increases knowledge about work

processes. The types of communication that occurs between co-workers, peers, or others may be the best evidence that knowledge transfer has occurred.

User participation in developing security training and awareness materials is one means to increase knowledge transfer among users of organizational security policies and is a core focus of this research.

2.2. User Participation

The concept of participation in decision making has been studied in the organizational behavior (OB) literature since the 1970's, and similarly studied as user participation in the information systems development (ISD) literature for just as long. Generally speaking, "participation implies that there is shared decision making. People contribute according to their competence and not necessarily by position" [28]. Within the context of ISD, user participation has been defined as the extent to which users or their representatives carry out assignments and perform activities and behaviors during ISD [29].

In both the OB and ISD literatures, participation has been most often associated with employee or user satisfaction and productivity, with mixed results from empirical studies. For example, in a review of 82 studies on user participation within the ISD literature, [30] found that user participation is minimally-to-moderately beneficial to ISD, and that its effects are comparatively stronger on attitudinal/behavioral outcomes than on productivity outcomes. One explanation for the mixed research results of participation's effects is that although participation has been widely studied as a means to gain acceptance and satisfaction, perhaps its most valuable contribution is cognitive rather than psychological. In particular, participation's greatest contribution may be through information exchange and knowledge transfer [31]. Indeed, user participation is considered to be a means to improve system design by eliciting more accurate system requirements and domain knowledge from users [30]. Thus, user participation has been found, to varying degrees, to influence user acceptance, satisfaction, performance, and quality.

More recently, user participation has been studied within the IS security literature. It has been suggested that increasing the user's role in IS security work may help to reverse the problems of a lack of user motivation and knowledge in IS security related work [15]. Indeed, in a study that examined user participation in the design and implementation of IS security controls, organizational awareness of security risks and controls within business processes increased, which in turn was found to contribute to more effective security control development and performance [32]. By assigning users hands-on security-related tasks within their business processes, security becomes more visible and relevant to them, and user knowledge of information use within their business processes aids the design of more effective security measures.

Within the context of security awareness programs within an organization, user participation in developing training materials may make training materials more relevant to users and their peers. It may also contribute to more effective design of security awareness materials. In addition, this participation is likely to result in information sharing and knowledge transfer among users, and thus, result in greater performance of security policies and procedures disseminated in the training. As such, we propose the following model.

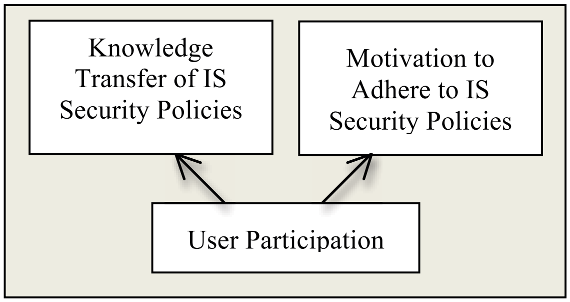
Knowledge Transfer of IS Security Policies
Motivation to Adhere to IS Security Policies
User Participation

Figure 1. User participation leads to knowledge transfer of IS security policies and adherence to IS security policies

Based on the model in Figure 1, our research question is, "Does user participation in the development of an IS security awareness campaign increase knowledge transfer among users of organizational IS security policies, and increase user motivation to adhere to IS security policies?".

3. Research Location

This research project was conducted at an institution of higher education that we call Mountain View University (MVU). MVU employs less than 600 faculty and staff members. Their IS security policies can be accessed from the university's website. MVU offers an IS security training to new employees during convocation week only. However, participation is not mandatory. As a result, many new employees choose not to participate in the training. These employees, however, are provided access to sensitive information to complete daily tasks.

4. Research Method and Data Analysis

Based on prior research, a users' absorptive capacity, disposition for motivation, and the training communication methods provided are likely to determine whether knowledge transfer will occur. This study drew from these three prior concepts on knowledge transfer and designed a multi-phase assessment in a case study location. The aim of the assessment was to communicate IS security to employees via means of two-way discussion and learning. Researchers believed MVU would act as a valuable case study location due to: 1) a general assumption that the absorptive capacity of employees within MVU would be adequate for this exploratory phase of work; and 2) findings from phase I of the study indicated MVU to be one of many common work environments where little IS security training had been provided or received. With little prior emphasis on IS security training, researchers determined that little work had been done at MVU to increase employee motivations in regards to transferring knowledge about IS security. As such, conducting this study at MVU would allow researchers to study a phenomenon that had not been previously assessed and where employee motivation could develop more naturally as a result of a lack of IS security training efforts.

The first phase of research was an exploratory study to check the above stated assumptions and determine end users' awareness of the university's IS security policy and their participation in any SETA programs available on campus. This phase was necessary to understand if users have existing knowledge of IS security policies and access to sensitive information. In addition, this phase provided information necessary to address knowledge transfer in the second phase. The second phase was conducted one month after the completion of phase one and included a user participation workshop for the development of an IS security awareness program on campus. Details of each phase are described below.

Phase One: User Awareness

An exploratory study involving an online survey of faculty and staff at MVU was performed to determine end users' awareness of the university's IS security policy, users' participation in a SETA program, and users' awareness of any IS security awareness programs on campus. To gain university participation, two email messages were sent to all employees asking for their participation in the study. The survey was available for two weeks by way of SurveyMonkey.com. One hundred twenty-eight faculty and staff members completed the survey.

According to Table 1 below, ninety-six or 75% of the respondents stated that MVU does have an IS security policy. Thirty-one (24.2%) of the respondents stated that they don't know if MVU has an IS security policy.

Table 1. Users who know if MVU has an IS security policy

Does MVU have an IS Security Policy?		
Yes	No	I don't know
75% (96)	0.8% (1)	24.2% (31)

Of those who stated that MVU has an IS security policy, only fifty-two (54.2%) stated that they read the policy and forty-three (44.8%) stated that they didn't. One participant stated that they didn't know.

MVU employs information systems to collect, store, and disseminate information that is protected by state and federal regulations. This information includes six different types: educational, financial, medical, personally identifiable information (PII), social security numbers (SSN), and usernames and passwords. Of the 128 research participants, 113 (88.3%) stated that they have access to and use sensitive information to complete daily and/or weekly tasks. Three (2.3%) of the respondents stated that they don't know if they do, and 12 (9.4%) stated that they don't (see Table 2).

Table 2. Users who have access to and use sensitive information to complete daily or weekly tasks

Do you have access to or use any of the following types of information to complete daily or weekly tasks?	**Response Count**
Educational – class schedule and grade information	(75.8%) 97
Financial – bank account, checking information and credit card numbers	(26.6%) 34
Medical – Medical information of an individual	(6.3%) 8
Personally identifiable – name, address, birth date, e-mail address, etc.	(75.8%) 97
Social security number (or the equivalent if the incident occurred outside of the United States).	(26.6%) 34
Usernames and passwords – Access credentials of an individual to information resources	(20.3%) 26
No	(9.4%) 12
I don't know	(2.3%) 3

Respondents were asked if they participated in an IS security training program that explained how to protect and safeguard sensitive information. As shown in Table 3 below, 31 (28.4%) marked that they have participated in a training program, and 74 (67.9%) stated that they have not participated in a training program.

Of the thirty-one respondents who stated that they participated in a training program at MVU, eighteen stated that they had training on FERPA, two stated that they had training about email usage, one had training about financial aid and social security numbers, and two others stated that they did not remember what type of training they had received.

Table 3. Users who participated in an IS security training program at MVU

Have you participated in a training program at MVU that explained how to protect and safeguard sensitive information?	
Yes	28.4% (31)
No	67.9% (74)
I don't know	3.7% (4)

Respondents were also asked if they received any information reminding them to protect and safeguard sensitive information. Ninety-two (84.4%) participants marked the affirmative; with most specifying that they had received information relating to FERPA. Eleven (10.1%) stated that did have not and six (5.5%) stated that they don't know if they received information reminding them to protect and safeguard sensitive information.

This first phase provided us with a general understanding of respondents' existing knowledge of IS security policies at MVU and their use of sensitive information to complete tasks. While practitioners at MVU sought to increase employee training efforts, researchers aimed to further understand how employee knowledge may improve through participating in the design of awareness programs. As such, a second phase of research was conducted to explore this concept. Phase I findings contributed to the development of materials used during phase two of this study.

Phase Two

Phase two of this research project was to bring together faculty and staff who have access to sensitive information (i.e., including directors, managers, or similar position from various departments) in efforts to develop an IS security awareness program on campus. The goal of this initiative was to determine if participants would transfer the knowledge they gained at an IS security awareness workshop to others. Participation in this ninety-minute workshop was voluntary, and was conducted during a time when most employees take their lunch break (12-1:30pm). Lunch was provided for all who participated.

With the help of the Human Resource Director and the Registrar, thirty-four people were identified as having access to sensitive information and were invited to attend the workshop. Of those invited, twenty-two people volunteered to participate. Table 4 provides a list of job titles of individuals whom attended.

Table 4. Research Participants

Research Participants
Accountant, Business Financial Services
Manager (3)
Assistant to the Dean, College of Business
Director (8)
Professor and Director of the Institutional Review Board
Program Associate, Dept. of Nursing
Records Staff (4)
Registrar
Student Advisor
Transfer/Degree Audit Specialist

At the beginning of the workshop, participants were shown a fifteen minute PowerPoint presentation that explained why they were invited to participate in the workshop, the state and federal regulations that serve to protect the information the university collects, types of IS security violations (malicious and non-malicious), reported data breaches in higher education [10], consequences of data breaches, and how to improve compliance with SETA and/or sanctions. Participants were then asked to complete a survey asking for information relating to their knowledge of the university's IS security policy and to determine if they witnessed, heard of, or accidentally disclosed information in violation of the university's IS security policy, or state and federal regulations. This questionnaire helped set the stage for a follow-on discussion and question and answer session.

All participants stated that they had received access to or had used information protected by U.S. state and federal laws and regulations to complete daily and/or weekly tasks. In addition, eighteen (86%) participants stated that they were aware of the university's IS security policies, but only four (18%) had read it (see Table 5).

Table 5. Participants' awareness of MVU's IS security Policy

Are you aware of MVU's IS Security policy	
Yes, and I have read it	18% (4)
Yes, but I have not read it	68% (15)
No, but I assume there is one	.091% (2)
No	.045% (1)

Participants were asked if they had ever witnessed, heard of, or even accidentally disclosed information in violation of U.S. state and federal regulations or MVU IS security policies. According to Table 6, 9 (41%) participants witnessed someone, 14 (63.6%) heard of another, and 9 (41%) accidentally disclosed information in violation of U.S. state and federal laws and regulations, and MVU's IS security policies.

Table 6. Disclosure of sensitive information

Witnessed, heard of, or accidentally disclosed information in violation of U.S. state or federal regulations, or MVU's IS security policy. Key - Motivation			
	Witnessed	Heard of	I accidentally
Yes	41% (9)	63.6% (14)	41% (9)
No	59.1% (13)	36.3% (8)	59.1% (13)

When asked if they participated in an IS security training program, 13 (59%) of the participants stated that they had and 9 (41%) stated they had not. In addition, not one had previously participated in the development of an IS security awareness program.

Researchers sought to understand motivations behind participating. As such, participants were asked, not including the invitation to participate, what motivated them to participate in the research study. One participant stated, that IS security is an "*important issue for MVU*." Six stated that they are interested in or curious about IS security. Another participant stated, "*the opportunity to be involved in something outside my own area/office*."

After all pre-surveys were completed, the participants were placed into groups based on their location in the classroom. Groups consisted of four or no more than five members. Groups had approximately 30 minutes to discuss the information they learned from the PowerPoint presentation, and come up with an IS security awareness program that they believed could be effective at MVU. The participants developed four different IS security policy and awareness program ideas. These ideas included:

1. The use of screen savers that are triggered by a "time-out"
2. Use of digital signatures
3. Mandatory training with a test
4. Employee monitoring

After the initial group meetings, participants gathered across groups to discuss security campaign ideas. In these discussions, participant's expanded upon earlier ideas and suggested several additional potential policies including:

5. Mandatory *online* training with a passing grade on a test
6. Ongoing mandatory training
7. 1 year *online* refresher training course
8. Train student workers
9. Instructor-led, face-to-face training
10. Pop-up screen savers with awareness tips

After each group shared their ideas to develop an IS security awareness program for campus use, participants discussed IS security issues on campus and asked one of the researchers questions. One question in particular was how to create a strong password. The researcher explained characteristics of a strong password and how to create strong, memorable passwords.

Phase Two - Post survey analysis

Two weeks after the workshop, participants were asked to complete an online survey about their participation in the workshop, if they shared information about the workshop with others, and if they were doing anything more to protect and safeguard sensitive information. Of the twenty-two participants who took part in the workshop, 18 complete the post survey.

Table 7. Participants who share knowledge of the workshop

Did you tell anyone about your participation in the IS security awareness meeting? Check all that apply. Key – Communication	Response Count
Supervisor/manager	22.2% (4)
Coworker	61.1% (11)
Family member	27.8% (5)
Friend	16.7% (3)
No	22.2% (4)

As mentioned previously, an important indicator that demonstrates that knowledge transfer has occurred is when participants communicate what they learned with other individuals. Participants stated that they shared information about the workshop with their supervisors/managers, coworkers, and family and friends. Four (22.2%) participants, however, stated that they did not share information with another individual (see Table 7).

It is important to differentiate whether participants merely communicated that they attended a workshop versus communicating what was learned while attending a workshop. To assess this, qualitative feedback was received from participants on what was communicated with others. In most cases, participants noted sharing the content of the workshop with others. For example, one participant stated that they shared, "the content of the class, and how to build and remember strong passwords." In this regard, the following responses were received from participants:

> "[I] discussed the need for personal IS Security - cell phones, pass words etc..."
>
> "I told them how important it is to have good passwords, and also I told my coworkers about using your computer at work with personal information, such as credit card numbers, bank account numbers, etc."
>
> I explained "How easy it is for people to gain access to your stuff if it is not secured..."
> "They [colleagues] were not aware of how confidential information can be easily accessed if not protected."
>
> "I talked with a friend about a strong password and how creative it was to create and remember a strong password."
>
> "I talked with [my colleague] about the meeting."

Additional evidence that knowledge transfer took place included communications from several participants encouraging others to participate in the workshop and/or to implement policies. For example, one staff member explained:

> "[I stated the workshop] would be good for other employees in our department."

Another participant related his/her interest in implementing what was learned:

> "All of my co-workers were there [at the workshop], so I didn't tell anyone about the training. However, we did talk about the training together and talked about possibly implementing some of the ideas."

As described earlier, knowledge transfer is influenced by the recipient's motivation to acquire new knowledge, assimilate it, and apply it. According to Table 8, 11 (61.1%) of the participants agree that because of their participation in the workshop they are doing more to protect and safeguard sensitive information. Others 7 (38.9%) stated that they somewhat agree.

Qualitative feedback was asked from participants to understand what they were doing to protect sensitive information. In this regard, the following responses were received from participants:

> "[I am] looking at the legal ability to remove some information from forms."
> "I printed new FERPA cards and posted at my workstudy stations."

Table 8. Participants who are motivated to protect and safeguard information

Because of my participation in the IS security awareness meeting, I am doing more to protect and safeguard sensitive data. Key - Motivation	**Response Count**
Agree	61.1% (11)
Somewhat agree	38.9% (7)
Somewhat disagree	0
Disagree	0

Although awareness and training to increase user compliance doesn't always require the end user to completely change business processes, it does encourage users to be more aware of the types of information they are working with and adopting practices to protect and safeguard that information when it is in use, stored, and at rest. In this regard, the following responses were received from participants:

> "I have not yet developed any new methods or anything. I just try to be very careful."
>
> "I am now highly sensitive to keeping information/documents confidential and secure."

5. Discussion

Based on prior research, a users' absorptive capacity, disposition for motivation, and the communication methods utilized are likely to determine whether knowledge transfer will occur [20; 21; 18]. This study drew from these three prior concepts on knowledge transfer to guide the design of a multi-phase assessment in a case study location (MVU). The aim of the study was to explore the potential that user participation in developing a security awareness program may also be a contributing factor for knowledge transfer to occur. This was studied within the context of an IS security awareness training program.

Given the results of the survey in phase one of this research we found that approximately 91% of the respondents had received access to and had used sensitive information to complete daily and/or weekly tasks. Considering a very well-known history that users have been identified as the weakest link in IS security management [33], it was alarming to find that only 28.4% of all respondents at MVU had participated in an IS security training program to understand how to protect and safeguard sensitive information. While 84.4% of university-wide respondents stated that they have received information reminding them to safeguard information protected by FERPA, they may not understand the importance of safeguarding personally identifiable information and information protected by HIPAA, PPRA and GLBA. This may be evident given the number of employees, who participated in phase two of this research, who witnessed and/or heard of someone, or they, themselves, accidentally disclosed information in violation of U.S. state and/or federal regulations or MVUs IS security policy.

Phase two of this study included a workshop where instructors and employees constructed an IS security awareness plan together. Individuals whom participated in the workshop shared information with each other relating to their work environment, provided insight as to how they believe the information they use to complete tasks could be better protected, and offered solutions to support IS security policies on campus. Participants were also found to communicate knowledge about IS security to others just days and weeks following the workshop. This communication took place informally and interpersonally with peers, co-workers, and family members. Consistent with [15], the workshop is an effective tool to influence user behavior and awareness toward IS security practices.

The motivation of employees to engage in knowledge transfer activities may have been influenced by their participation in the design workshop. This is evident in respondents' post-workshop responses that indicated taking steps, or actions, to safeguard sensitive information and communicate knowledge gained from the workshop with others. This is consistent with [32] who reported that organizational awareness of security risks and controls within business processes increased when users participated in the design and implementation of IS security controls. Therefore, user participation in a design process may be an important ingredient for knowledge transfer about IS security to occur.

While the literature [20; 21; 18] discusses motivation and communication as components of knowledge transfer, our findings suggest that user participation in the development of an IS security awareness program can generate knowledge transfer of IS security policies and procedures and can motivate users to adhere to IS security policies. This is depicted in Figure 2.

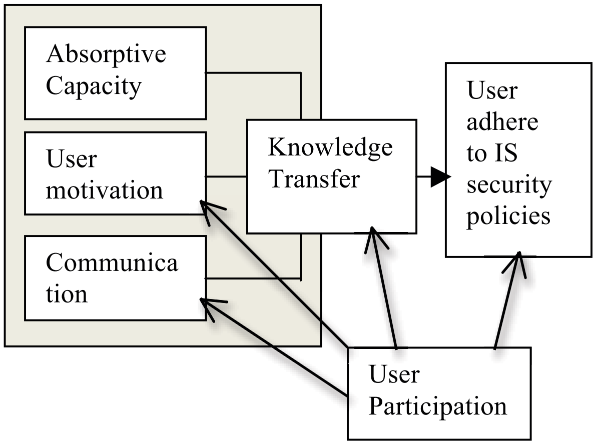

Figure 2. User participation for the transfer of knowledge to increase adherence to IS security policies

6. Limitations and Future Research

This research was performed at a state university in the western United States (U.S.). Therefore, future research is needed to study user participation in the development of IS security awareness campaigns at universities of different sizes, and in other parts of the U.S. and in other countries. It would also be valuable to conduct a modified version of this research across different types of organizations using appropriate security training to those settings (i.e., Healthcare, Business). Furthermore, MVU was operating during a time of financial difficulty. Higher education institutions operating in a more stable business environment may generate different results. As such, future research is needed to explore user participation in the development of IS security awareness programs in institutions of higher education that are operating in a more stable environment.

MVU employs less than 600 employees, and although all employees were asked to participate, only 128 employees completed phase one's online survey. Participation from additional employees could have generated different results. In addition, the authors asked 34 employees, who were identified by MVU's HR director and registrar as having access to sensitive information, to participate in the IS security awareness workshop. Only 22 participated. Results of this study may be different if more employees participated in the study. For example, those who didn't participate in the study may know about and have participated in awareness programs.

While a major limitation of this study is its small pilot scale and exploratory focus, a next phase of research should further investigate how user participation in a design process impacts knowledge transfer. A future quantitative study instrument should take into account the concepts noted herein (absorptive capacity, motivation, communication) in regards to knowledge transfer. Furthermore, the focus of this study has been on the context of IS security specifically. In this regard, a common and important outcome for IS security training is user adherence to IS policy. As such, a future study should also aim to assess how knowledge transfer and participation are achieved and result in adherence to IS policy. As such, the model shown above in Figure 2 is preliminary and should be used for future development and testing.

7. Conclusion

Institutions of higher education are required to protect and safeguard sensitive information in accordance with state and federal laws and regulations. Many organizations, including institutions of higher education, have implemented methods to ensure institutional compliance. Unfortunately these methods, including SETA programs, have been less than effective and data breaches due to insider threats continue to be on the rise.

This case study proposes a different approach to increase user compliance to organizational IS security policies to safeguard information that is protected by state and federal regulations; user participation. The results of this study suggests that users who participate in a workshop to develop an IS security awareness and training program are likely to communicate knowledge about IS security policies to others, and be motivated to apply the new knowledge when completing daily tasks. Further, employing a workshop, or the like, to promote user participation in IS security initiatives provides users an opportunity to gain fundamental knowledge of IS security policies and practices and promotes collaboration among users by sharing ideas that could help them to be more compliant in their jobs. Gaining fundamental IS security knowledge in a workshop-based environment may enhance end users' ability, or the absorptive capacity, to process new information from additional IS security initiatives. Thus, this research presents an example of how factors of knowledge transfer coupled with user participation can promote adherence to IS security policies.

8. References

[1] S. Grajek, S. "Top-Ten IT issues, 2013: Welcome to the Connected Age", EDUCAUSE Review, Vol. 48(3), 2013. Retrieved on June 10, 2013 from http://www.educause.edu/ero/article/top-ten-it-issues-2013-welcome-connected-age.

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

[3] A.C. Johnson and M. Warkentin, M. "Fear Appeals and Information Security Behaviors: An Empirical Study", MIS Quarterly, Vol. 34(3), 2010, pp. 549-566.

[4] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance, "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study", European Journal of Information Systems, Vol. 18(2), 2009, pp. 126-139(14).

[5] A. Vance and M. Siponen, "IS Security Policy Violations: A Rational Choice Perspective", Journal of Organizational & End User Computing, Vol. 24(1), 2012, pp. 21-41.

[6] D.W. Straub, "Effective IS Security: An Empirical Study", Information Systems Research, Vol.1(3), 1990, pp. 255-276.

[7] R. Willison and M. Warkentin, "Beyond Deterrence: An Expanded View of Employee Computer Abuse", MIS Quarterly, Vol. 37(1), 2013, pp. 1-20.

[8] T. SanNicolas and L. Olfman, "End User Security Training for Identification and Access Management", Journal of Organizational and End User Computing, (Forthcoming), 2013.

[9] M. Warkentin, J. Johnson, and J. Shropshire, J, "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and

Intention", European Journal of Information Systems, 20, 2011, pp. 267-284.

[10] Privacy Rights Clearinghouse. Retrieved on June 8, 2013 from https://www.privacyrights.org/data-breach/new.

[11] G. Dhillon and T. Moores, "Internet Privacy: Interpreting Key Issues", Information Resources Management Journal, Vol. 14(4), 2001, p. 33.

[12] E.D. Shaw and H.V. Stock, "Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall", White Paper, Symantec, Mountain View, CA, 2011.

[13] PwC, "The Global State of Information Security Survey 2013". Retrieved on June 2, 2013 from http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf.

[14] M. Karjalainen and M. Siponen, Toward a New Meta-Theory for Designing Information Systems Security Training Approaches", Journal of the Association for Information Systems, Vol. 12(8), 2011, pp. 518-555.

[15] E. Albrechtsen, "A Qualitative Study of Users' View on Information Security," Computers & Security, Vol. 26, 2007, pp. 276-289.

[16] B.D. Cone, C.E. Irvine, M.F. Thompson and T.D. Nguyen, "A Video Game for Cyber Security Training and Awareness", Computers and Security, Vol. 26, 2007, pp. 63-72

[17] NIST SP 800-16, National Institute of Standards and Technology (NIST). "Information Technology Training Requirements: A Role- and Performance-Based Model (NIST Special Publication 800-16)", Washington, DC: US Department of Commerce, 1998.

[18] M. Alavi and D. Leidner, "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues", MIS Quarterly, Vol. 25(1), 2001, pp. 107-136.

[19] I. Nonaka, "A Dynamic Theory of Organizational Knowledge Creation", Organization Science, Vol. 5(1), 1994, pp.14-37.

[20] K. Ko, L. Kirsch and W. King, "Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations", MIS Quarterly, Vol. 29(1), 2005, pp. 59-85.

[21] A. Gupta and V. Govindarajan, "Knowledge Flows Within Multinational Corporations," Strategic Management Journal, Vol. 21, 2000, pp. 473-496.

[22] P. Puhakainen and M. Siponen, "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study", MIS Quarterly, Vol. 34(4), 2010, pp. 767-A4.

[23] W. Cohen and D. Levinthal, "Absorptive Capacity: A New Perspective on Learning and Innovation", Administrative Science Quarterly, Vol. 35(1), 1990, pp. 128-152.

[24] R. Clark, "A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation", The 2nd Multidisciplinary Workshop on Identity in the Information Society, LSE, 5, 2009.

[25] M. Ziemba, "A Training Framework for the Department of Defense Public Key Infrastructure", Unpublished Master's Thesis, Naval Postgraduate Institute, 2001.

[26] D.L. Goodhue and D.W. Straub, "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security", Information & Management (20), 1991, pp.13- 27.

[27] D.W. Straub and R.J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making,"MIS Quarterly, Vol. 22(4), 1998, pp. 441-469.

[28] T.R. Mitchell, "Motivation and Participation: An Integration", Academy of Management Journal, Vol. 16(4), 1973, pp. 670-679.

[29] J. Hartwick and H. Barki, "Explaining the Role of User Participation in Information System Use", Management Science, Vol. 40(4), 1994, pp. 440-465.

[30] J. He and W.R. King, "The Role of User Participation in Information Systems Development: Implications from a Meta-Analysis", Journal of Management Information Systems 25(1), 2008, pp. 301–331.

[31] E. A. Locke, M. Alavi and J.A. Wagner III, "Participation in Decision Making: An Information Exchange Perspective", Research in Personnel and Human Resources Management, Vol. 15, 1997, pp. 293-331.

[32] J. Spears and H. Barki, "User Participation in Information Systems Security Risk Management", MIS Quarterly, Vol. 34(3), 2010, pp. 503-522.

[33] K. Guo, Y. Yuan, N.P. Archer and C.E. Connelly, "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model", Journal of Management Information Systems, Vol. 28(2), 2011, pp. 203-236.