Knowledge Retention in Information Assurance Training: A Case Study of Security Awareness Training in University Environment

Jing Yang

Management Science and Information Systems
William S. Spears School of Business
B-04 SSB, Oklahoma State University
Stillwater, Oklahoma 74078
405-744-4078
jing.yang10@okstate.edu

David Biros

Management Science and Information Systems
William S. Spears School of Business
Oklahoma State University
415 Business Building
Stillwater, OK, 74078-4011
405-744-7156
david.biros@okstate.edu

Michael Hass

Management Science and Information Systems
William S. Spears School of Business
B-04 SSB, Oklahoma State University
Stillwater, Oklahoma 74078
405-744-3983
michael.hass@okstate.edu

ABSTRACT

With the development of information technologies (ITs), the challenges from information security are becoming more and more non-ignorable. Researches demonstrate that a great part of information security problems are caused by human beings. In addition to the improvement on ITs, the outcome of effort on reducing human errors is also outstanding. In this paper, we put focus on users' security awareness. Our purpose is to explore the relationship between security training and knowledge retention. An experiment is designed according to the conceptual model provided in the paper. The future work of research also will be discussed in the end.

KEYWORDS

Information Security Training, Security Awareness, Knowledge Retention

INTRODUCTION

Information security issues have attracted researchers' attention for a long time. According to Welke (1998)'s definition, a security incident could refer to the situations that data, records, files, program, or computer hardware have been improperly and deliberately used, modified, destroyed, stolen, or damaged (Welke, 1998). With the development of information technologies (ITs), the variety of security threats increases dramatically which makes the protection of private information more complex and challenging in turn. The "information security breaches survey 2004", conducted by British Department of Trade and Industry in association with Price Water House Coopers, discovered that insider misuse had doubled since the year 2002, which was mainly driven by the increased adoption by WWW and Internet related technologies (Magklaras & Furnell, 2005). In Whitman' research (2003), the Act of Human Errors or Failure was ranked first among all the threats. Particularly as for the number of attacks per month, 5.2% responders thought they made error or failures more than 100 times per month, 2.1% between 51 to 100 times, 14.6% between 10 and 50 times, and 41.7% less than 10 times. Later Knapp et al (2006) did another survey to discuss the top information security issues facing organizations. They ranked a list of 25 information security issues based on which one were the most critical facing organization today(Knapp, Marshall, Rainer Jr, & Morrow, 2006). The top five rankings in their study were top management support, user awareness training and education, malware, patch management, vulnerability and risk management. The detailed information is presented in Table1. Although the emphases of the surveys were different, we still can tell that the security threats which are caused by human factors are still severe, and the need of user awareness training and education is ranked high.

Table 1. Top Ten Security Issues

Rank	Whiteman (2003)	Knapp (2006)
1	Act of Human Error or Failure	Top management support
2	Compromises to Intellectual Property	User awareness training & education
3	Deliberate Acts of Espionage or Trespass	Malware (e.g. Viruses, Trojans, worms)
4	Deliberate Acts of Information Extortion	Patch management
5	Deliberate Acts of Sabotage or Vandalism	Vulnerability & risk management
6	Deliberate Acts of Theft	Policy related issues (e.g. enforcement)
7	Deliberate Software Attacks	Organizational culture
8	Forces of Nature	Access control & identity management
9	Quality of Service Deviations from Service Providers	Internal threats
10	Technical Hardware Failures or Errors	Business continuity & disaster preparation

As mentioned above, the effect of human factor on the security threats has been paid attention for a while. For example, Cone et al. (2007) found that cyber security training and awareness was considered one of five areas of highest priority for action in a national plan for cyberspace security, and the enormity of the problem associated with effective user training and awareness is its powerful evidence (Cone, Irvine, Thompson, & Nguyen, 2007). Security training also has been identified to be a good tool to help users have the better understanding of the threat(Charoen, Raman, & Olfman, 2007). Lytras (2008) pointed out that the knowledge management mechanism and security issues have a mutually effect on each other. Knowledge management could work as a good theoretical guideline to the security issues, which are highly correlated to the technologies (Lytras, 2008). So an effective user security awareness training could greatly enhance the information assurance posture of an organization (Cone et al., 2007).

In this study, our purpose is to explore the relationship between users' security awareness and knowledge retention. Besides, by summing up the past research, we also want to figure out the factors which affect the outcome of security knowledge training. In general, this paper mainly contains four parts. Except the introduction, in part two, we will articulate our conceptual model in the research. In part three, the corresponding experiment design will be briefly explained. And finally, our study in the next step will be discussed.

CONCEPTUAL MODEL

Based on the past research, it is believed that users' awareness of information security is associated with training modality, training amount, testing recurrence and computer literacy. Besides, there is relationship between awareness of information security and knowledge retention, knowledge retention and time. The concrete relations and hypotheses are presented in Figure 1.

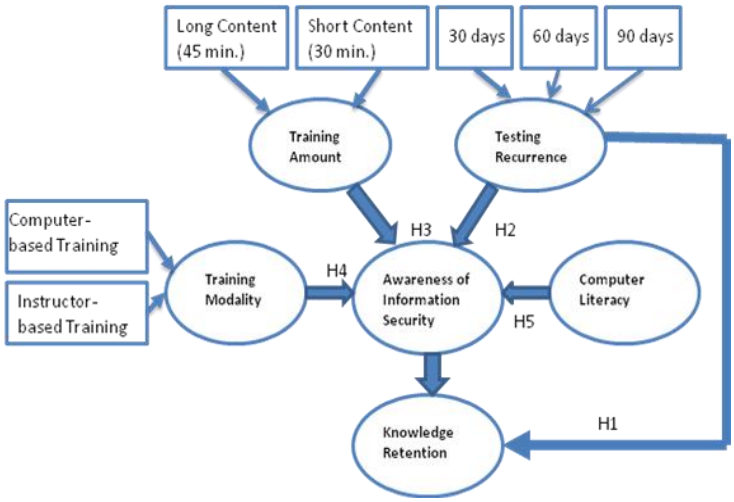

Figure1. Conceptual Model

Knowledge Retention

Technically, knowledge retention could be defined as the loss of decay of trained or acquired skills (or knowledge) after extended periods of time(Casper, 2008). In psychology, people thought the way how knowledge retention works is associated with types of memory failure. In general, the memory failures could be categorized in three ways(Brigman, 2004). The first type of forgetting is named as short-term forgetting, which refers that people forgot information at a later time after encoding. The second type of forgetting is named as long-term forgetting, which refers people forgot information at a later time. And the last type of forgetting is named as very long-term forgetting, which refers that people forgot highly familiar and over-learned information.

Besides, knowledge retention is also found related to learning cycle. In order to know the cycle of learning and memory, several experiments have been done over animals, such as rats. For example, Wiltgen et al. (2007) have conducted one experiment over rats to determent whether changes in generalization over time are due to a loss of details for context memory, and whether a reminder treatment could reduce generalization at remote time points and restore the specificity of context fear. In that experiment, they found that memory for context becomes less specific over time, and a reminder treatment could restore context discrimination(shown in Figure and Figure)(Wiltgen & Silva, 2007). This kind of thought is consistent with the types of memory failure. Although in this study our targets are human beings, this pattern of research still could be introduced into our experiment. Differently, it will be embodies by test recurrence and time passing by in the experiment.

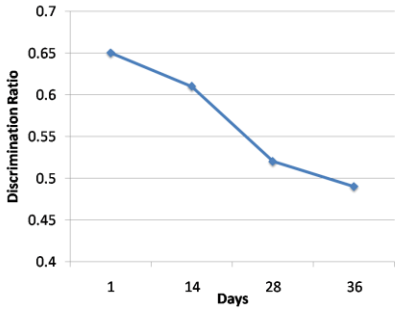

Figure 2. Memory for Context over time
Adapted from Wiltgen (2007)

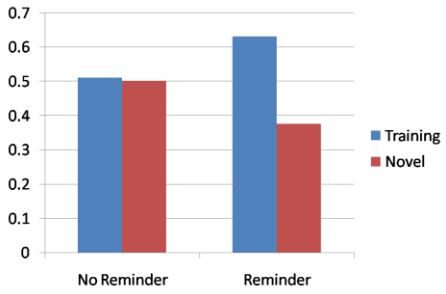

Figure 3. Comparison between Reminder Treatment and Non reminder Treatment
Adapted from Wiltgen (2007)

To sum up, the hypotheses involved in this part could be as follows:

H1: Information security knowledge decreases with time passing by.

H2: Testing recurrence has a positive effect on awareness of information assurance.

Information Security Training

In this section, the training issues will be discussed from the perspective of educational psychology. First of all, the outcome of training is associated with communication tools, which are fundamental to training programs. Traditionally, communication tools in training refer to face-to-face, work collaboration, telephone, or voicemail(Lytras, 2008). With the development of modern technologies, email, video, video game, or other electronic (Net) communication methods could be adopted (Lytras, 2008). Their relationship is presented in Figure 4. In Figure 4, the methods on the right side are more electronic than those on the left side, which are comparatively more conventional. In this study, we are going to use two opposite training channels – computed based training and instructor-led training. By comparing the outcome of them, the efficiency of these two channels will be tested.

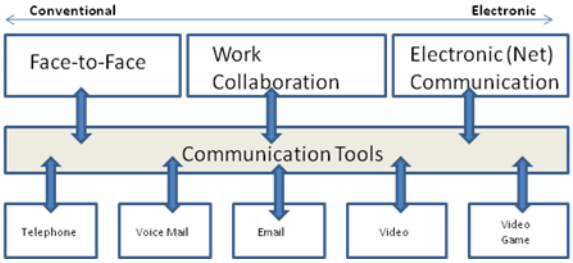

Figure4. Communication Tools. Note: Adapted from (Lytras, 2008)

As well, volume and intensity are thought to be two critical variables in periodized training program (Holiday, Burton, & Sun, 2008). Here training volume refers to the amount of work, while training intensity describes the quality of work produced. Figure5 and 6 present the volume-intensity crossover effects for training sports and team sports (Holiday et al., 2008). Besides, speed and accuracy is another consideration. Arthur and Bennett et al. (1998) insisted that the distinction between speed and accuracy as indicators of performance has been compared with the quantity versus quality distinction in the organizational psychology literature (Arthur Jr, Bennett Jr, Stanush, & McNelly, 1998). It was expected that speed tasks would display less knowledge decay than accuracy tasks. Similarly, although the past research worked on the sport training or something else, here we also want to adopt the idea on information security training, which is embodies by different training patterns discussed later.

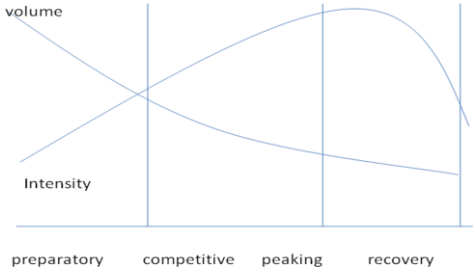

Figure5 Volume-Intensity Crossover Effects for Training Sports

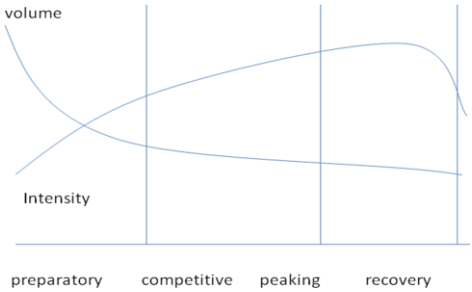

Figure6 Volume-Intensity Crossover Effects for Team Sports

Another important factor in training is the trainees. It is believed that different background of trainers also has an effect on the outcome and training and knowledge retention. For example, the age of trainees is a critical factor of memory failure. It has been proven that the time and pattern of forgetting are significantly different between younger (ranging in age from 18-32 years) and older (ranging from 63-81 years) targets (Brigman, 2004). In this study, a survey is designed to check trainees' background on computer literacy.

To sum up, the hypotheses involved in this part could be as follows:

H3: Training amount is positively related to awareness of information assurance.

H4: Training modality has a positive effect on information security knowledge.

H5: Trainees' computer literacy has a positive effect on information security knowledge.

RESEARCH DESIGN AND METHODOLOGY

The population of interest is normal computer users. This study employs two different training channels – CBT and ILT. In this study, 500 college students from MSIS department at Oklahoma State University will volunteer to attend the experiment. The data will be collected in February 2009. Both sections contain two different length of training content. The short training includes content for 30 minutes, while the long training includes content for 45 minutes. The long training is developed based on the short training. The difference emanates from how much details contained under each subjects.

Before training, a questionnaire will be distributed to measure whether the trainees' computer literacy impacts the outcome of training. A quiz will be immediately distributed after the training, which is treated as baseline. The expected score is above 70% of correctness. If the outcome of training is not satisfactory, a re-training will be offered. After the baseline quiz, three quizzes will be given to test on the level of knowledge retention. At this point, without consideration of majors, all the students will be divided into three groups based on different training channels and different training content. That means we will have 12 groups of student. To some extent, this is a 2x2x3 factorial experiment (as shown in Table 2). In order to measure how this relationship works in our scenario, the first group people will be given 3 quizzes with the frequencies of 30 days, the second group will be given 2 quizzes, and the third group will be given only one quiz (as shown in Table 3).

Table2. The Framework of Post Test

The length of Training / Means of Training	Short Content			Long Content		
CBT	G11	G21	G31	G13	G23	G33
ILT	G12	G22	G32	G14	G24	G34

Table3. The Framework of Training Recurrence

group \ days	30	60	90
G1			
G2			
G3			

Particularly, the questionnaire used in the study will briefly contain four sections. First of all, demographics will be included, because the literature shows the gender or age of trainees has an effect on the outcome of training. Secondly, questions of computer attitude will be asked, because if the trainees have a negative attitude toward computer, they probably will resist learning new information on computer. Finally, the information about trainees' information assurance experience and computer experience will be collected, because if they have a good experience on these two fields, probably their outcome of training could be much better than the other people. The concrete structure of questionnaire is presented in Figure 7.

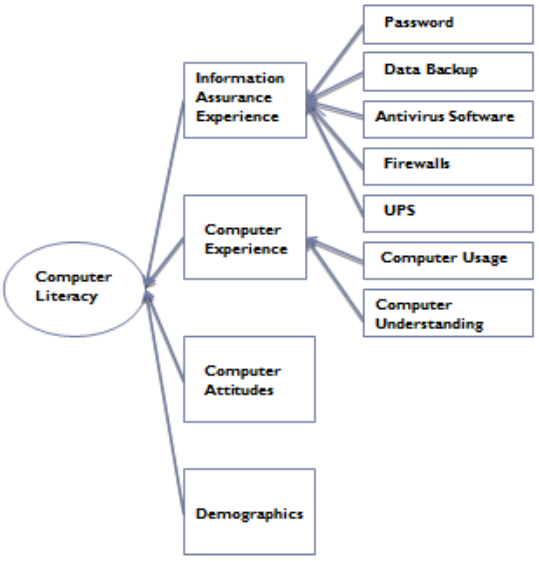

Figure7. Structure of Questionnaire

4. DISCUSSION

Another important component of training is its training content. Basically, in the training, we plan to cover the critical topics, such as laws and regulations, the organization and IT security, system interconnection and information sharing, sensitivity, risk management, management controls, operational controls, and technical controls. Particularly, the training will contain six models. In module 1, the reliance on IT systems and increased vulnerabilities of interconnected

systems and shared data will be introduced. In module 2, the importance of information will be discussed by talking about PII, FOUO, mobile devices etc. In module 3, the topics of importance of information assurance, such as CIA model and risk management, will be covered. In module 4, applied threats, such as insider/outsider, hacking/phishing, social engineering, viruses etc., will be demonstrated. In module 5, user responsibilities will be clarified. The topics such as password controls, safe practices, antivirus software and patches will be introduced. Finally, module 6 will cover personal and home computer security. Trainees will be taught how to deal with identity theft, E-commerce vulnerability, security home computer etc. This is only a brief construct of the training content. How to organize the content and make it efficient is one part of our future work.

Another problem we are facing is what methods we could use to analyze the data collected. In this study, we will get data out of the questionnaire and three quizzes. Consistent with the hypotheses involved in the conceptual model, the process of data analysis will be divided into three steps. At first, with respect to computer literacy, we plan to apply confirmative factor analysis to the outcome of questionnaire, and then use cluster analysis to classify the level of our trainees' computer literacy. Then use ANOVA or t test to compare the relationship between Computer-based Training and Instructor-led Training, Short Content and Long Content, or 30 days and 60 days and 90 days testing recurrence. Finally use factor analysis to test on the effects of each construct on knowledge retention. This will be an important step in our future work.

REFERENCE

Arthur Jr, W., Bennett Jr, W., Stanush, P. L., & McNelly, T. L. (1998). Factors That Influence Skill Decay and Retention: A Quatitative Review and Analysis. *Human Performance, 11*(1).

Brigman, S. K. J. (2004). *The Effect of Memory Knowledge on Attributions of Forgetfulness in Younger and Older Adults.* Louisiana State University.

Casper, E. S. (2008). Using Implementation Intentions to Teach Practitioners: Changing Practice Behaviors via Continuing Education. *Psychiatric Services ' ps.psychiatryonline.org ', 59*(7).

Charoen, D., Raman, M., & Olfman, L. (2007). Improving End User Behaviour in Password Utilization: An Action Research Initiative. *Systemic Practice and Action Research, 21*(1).

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A Video Game for Cyber Security Training and Awareness. *Computer & Security, 26*.

Holiday, B., Burton, D., & Sun, G. (2008). Building the Better Mental Training Mousetrap: Is Periodization a More Systematic Approach to Promoting Perform. *Journal of Applied Sport Psychology, 20*(2).

Knapp, K. J., Marshall, T. E., Rainer Jr, R., Kelly, & Morrow, D. (2006). The Top Information Security Issues Facing Organizations: What Can Goverment do to Help? *EDPACS, 34*(4).

Kuo, C., Perrig, A., & Walker, J. (2006). Designing an Evaluation Method for Security User Interfaces: Lessons from Studying Secure Wireless Network Configuration. *Interactions, 13*(3).

Lytras, M. (2008). *Knowledge Management Strategies: A Handbook of Applied Technologies*: Idea Group Inc (IGI).

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophiscation for insider threat prediction in IT systems. *Computers & Security, 24*.

Welke, D. W. S. a. R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4).

Wiltgen, B. J., & Silva, A. J. (2007). Memory for Context Becomes Less Specific with Time. *Learning & Memory, 14*.