https://doi.org/10.48009/1_iis_2012_215-224

Issues in Information Systems

Volume 13, Issue 1, pp. 215-224, 2012

MEASURING THE EFFECTIVENESS OF INFORMATION SECURITY TRAINING: A COMPARATIVE ANALYSIS OF COMPUTER-BASED TRAINING AND INSTRUCTOR-BASED TRAINING

Philip Kim, Walsh University, pkim@walsh.edu
Joseph V. Homan, joehoman3@gmail.com

ABSTRACT

Financial institutions are increasingly finding difficulty defending against information security risks and threats, as they are often the number one target for information thieves. An effective information security training and awareness program can be a critical component of protecting an organization's information assets. Financial institutions have invested significant resources in implementing information security training and awareness programs, but few have explored deeper to examine the effectiveness of these training programs. The purpose of this study was to examine the effectiveness of an information security training and awareness program within a mid-sized financial services institution. Effectiveness of information security training was determined by levels of knowledge transfer and knowledge retention. Additionally, the study was designed to determine whether the implementation of two different modes of training delivery, Instructor-based Training (IBT) and Computer-based Training (CBT) led to different results of effectiveness. The results indicate that instructor-based trainees had higher levels of knowledge transfer while the computer-based trainees had a higher level of knowledge retention within the 60-day time period. However, there was no statistically significant difference in 90-day knowledge retention rates within either IBT or CBT groups.

Keywords: Information Security, Training, Computer-based Training, Knowledge Retention, Knowledge Depreciation

INTRODUCTION

Information and data are widely accepted as the currency of today's economy [23]. Information systems and technologies that house an organization's most critical data are increasingly relied upon to provide information in a fast and efficient manner. The ability to provide speedy and accurate information can often be the difference between being a market leader or a market laggard [12]. Whitman and Mattord [30] argue that secure and accurate information is a necessity for organizations to attain their strategic business objectives.

The development of information technology (IT) and the accelerating growth of the Internet have brought with them a rapid increase in the use of open and shared network systems which improve the ability to provide immediate access to data [4]**.** As more customers have become technology-savvy, companies have grown increasingly dependent on their IT systems to provide services in more efficient and productive ways. IT advancements benefit both consumers and service providers, but they also demand an increase in secure management of information to reduce risks of service interruptions, theft, or alteration of data [13]. Accompanying the advance of the Internet technologies and the tech-savvy consumer is the increase in information security breaches and attacks on corporate networks [28]. Consequently, ensuring the confidentiality, integrity and availability of information has become a significant concern for both consumers and corporations [8]. Security technology systems such as firewalls, anti-malware applications, intrusion prevention and detection systems, and patch management systems are crucial to securing local and wide area networks. However, enhancing the overall information security environment involves more than simply investing in the latest security technologies. Even with the advancement of security technologies, the trend of information security breaches continues upward [29]. Many companies have implemented technology-related information security controls, however their attempts to protect information systems have often failed not due to the technology in place, but rather because of human error, end-user abuse, or fraud [10, 14]. In order to minimize the risks of human error, abuse, and fraud, organizations must provide adequate information security training. Formal information security training can provide reasonable assurance that employees will be equipped with the skills to act responsibly and practice safe computing habits [15, 21].

Financial Institutions

Information security is an important topic not only within the IT world, but has become especially relevant within the financial services industry. According to the 2007 CSI Security Survey [6], the number one target for Internet attacks and fraud attempts are financial service providers. Information thieves and hackers are constantly attempting to breach financial information systems, databases and business accounts. With the widely accepted use of Internet Banking, transactional websites, and online payment solutions banks are often the target of profit-minded technology thieves and hackers [27]. Banks rely heavily on IT to provide immediate and accurate service to their customers. Information is becoming more readily available and yet Porter and Millar [22] argue that because of the abundance of information availability, companies must find ways to ensure the information is credible and accurate in order to have a significant advantage over other organizations. Banks have increasingly placed an emphasis on IT to ensure that financial information and data are readily available when it is requested by customers or needed by the managers to make strategic business decisions.

Problem Statement

Financial institutions are increasingly finding difficulty defending against information security risks and threats. Siponen [26] explains financial institutions are often the number one target for information thieves and because of limited technical and human resources, many banks are not prepared to protect against information security threats. While many financial institutions have invested significant resources in implementing information security training and awareness programs, few have explored deeper to examine the effectiveness of these training programs.

Purpose of the Study

The purpose of the study was to examine the effectiveness of an information security awareness program within a mid-sized financial services institution. For the purposes of this study, the company will be referred to as ABC Bank. Effectiveness of ABC Bank's information security training program will be determined by the level of increase in information security awareness, or transfer of knowledge, and the ability of the trainee to retain the knowledge of information security awareness standards, or knowledge retention. Additionally, the study was designed to determine whether ABC Bank's implementation of two different modes of training delivery, Computer-based Training (CBT) and Instructor-based Training (IBT) led to different results in the transfer of knowledge and knowledge retention.

Theoretical Framework

The theory of adult learning [18] is important to this study because the field work focuses on the adult learning and educational experience. The participants in this study are adult employees of ABC Bank. Knowles [18] argues that the adult learning experience is dissimilar to the child learning experience, and therefore should be studied in contrast to existing child-based learning research. Knowles [19] explains the adult learning experience draws from the participants experience and existing knowledge. The adult learner is active and self-motivated to pursue learning or education, while the child learner is passive and needs to be prodded to learn [19]. Knowles' [19] adult learning model of learning was used to construct the face-to-face training seminar. Both computer-based training and instructor-based training modules were used in this study and measures were taken to determine differences in information security awareness and retention based on the different training methods.

Argyris and Schon's [2] Organizational Learning Theory provides another framework to measure how employees within an organization learn. These researchers explain that employees of an organization learn in different stages or phases. After learning the training material, employees adjust and modify their actions according to the difference between expected and obtained outcomes. As the individuals within the organization learn, their learning behavior adjusts to individual needs as well as organizational needs [2]. Donald Kirkpatrick's [16] model proposes a four-level method to evaluate training effectiveness. The first level is "reaction" or, what is the trainee's initial response to the training intervention? The second is "learning," that is, to what level was information transferred to the

trainee? The third is "behavior" or, did the training result in a change of behavior? And last is the "result." Did the training accomplish the organizational intent? The original model and derivations of the Kirkpatrick model have been used to measure the impact of corporate training programs [1, 20].

RESEARCH DESIGN AND METHODOLOGY

An experimental, quantitative research design was used to gain an objective measure of the effectiveness of the bank's information security awareness program. For the purpose of this study, effectiveness of the information security awareness program has been operationalized as trainee performance on post-training knowledge examinations based on mode of training delivery. The quantitative approach was utilized to collect and compare data results such as pre- and post-training results. The information security awareness program within this study included two modes of information security training which contained identical training material.

Overview of the Organization

The organization in this study is a financial service institution located in western Pennsylvania. The bank has over $5 billion in assets, is comprised of over 50 branches, and employs over 800 full-time employees and over 100 part-time employees. The bank has implemented mandatory annual corporate training initiatives for all employees.

Employees were asked to choose either CBT or IBT, as they were only able to participate in one training session. Prior to the training sessions, the primary researcher administered a pre-test knowledge quiz to determine the current level of information security knowledge prior to training. After the training session was completed the participants were asked to complete a post-test knowledge quiz. The post-test quiz results were compared to the pre-test quiz results to determine if there was any impact in the level of information security knowledge as a result of the training session. Both CBT and IBT participants received the same pre- and post-tests. The results of the pre- and post-test quizzes were compared based on the mode of training received.

The data collected included a demographic questionnaire, pre-post test examinations, and a post-test satisfaction survey. The independent variables were the two different training modes. The dependent variables were the two 10-question post-test examinations (short-term and long-term), individual and aggregate post-test examination scores, the demographic data including, age, gender, and job title.

60 and 90 Day Post-Test

Two post-test examinations were administered. The short term post-tests were administered immediately upon the completion of the training sessions for both CBT and IBT. The long term post-tests were administered to both the CBT and IBT participants to determine the level of knowledge retained by the participants. Approximately half of the long term post-tests were sent out to the participants 60 days after their training session. The remaining long-term post-tests were sent out 90 days after the completion of the training session. The independent variables were the two different training modes. The dependent variables were the individual and aggregate 60 and 90-day post-test results. The long term post-test results were utilized to measure the difference in the level of knowledge retained over an elapsed period of time.

Participants

The information security awareness program is mandatory for all full-time employees and optional for part-time and temporary employees. The population of this study was 212 full-time employees of the organization. There were 85 employees who volunteered to take part in the study by participating in the instructor-based training sessions and 127 employees who chose computer-based training sessions.

Instrumentation

The computer-based training module was developed by BVS Training Solutions Incorporated (BVS), a leading training and development company that specializes in providing training solutions. The CBT module utilized for this study is a BVS training course entitled Information Security Basics Course 2009 - STB 158. The BVS training instructional design principles are modeled to American Society of Training and Development standards but also according to proprietary adult learning design guidelines developed by BVS over 30 years of curriculum development in financial services and other industries. Specifically for the Information Security Course, BVS followed Federal Financial Institution Examination Counsel guidelines for financial institutions and the National Institute of Standards and Technology (NIST) guidance for information security guidance.

FINDINGS AND DISCUSSION

The objective of this research was to determine if employees who participated in traditional instructor-based information security training yielded comparable knowledge outcomes to employees who participated in computer-based information security training sessions. A secondary objective of this study was to determine if mode of training delivery has an impact on knowledge retention.

This section provides tabular, graphical, and narrative information of the results of the two modes of information security training delivery, IBT and CBT. The data were collected from participants of both methods, including pre- and post-test quizzes, a satisfaction survey, and a demographic questionnaire. Prior to participating in the information security training session, all participants completed a pre-test. The pre-test score was based on the number for correct questions on a 10 question knowledge quiz. After completing the training session, participants were asked to complete a post-test and a satisfaction survey. The dependent variables were the post-test scores and satisfaction survey results, while the independent variables were the mode of delivery for information security training program.

Participant Characteristics

A total of 212 employees participated in either the IBT session (code = 1) or the CBT training session (code = 2). As table 4.1 shows, 85 employees chose to participate in the IBT session for 40.1% of the study population, while 127 employees participated in the CBT session representing 59.9% of the study population. Other characteristics such as age, gender, job title, and previous participation in the BVS information security training session were collected via demographic survey.

Table 4.1: Demographics of Study Population

Demographic Information	Instructor-based Training Group:	Computer-based Training Group:	Both IBT and CBT Groups:
Participants:	n = 85	n = 127	212
Percentage:	40.10%	59.90%	100.00%
Mean Age:	41.2	45.5	43.8
Gender:			
Male:	38.80%	45.70%	42.90%
Female:	61.20%	54.30%	57.10%
Modal Job Title:	Branch Manager (n=15)	Personal Banker (n=17)	Personal Banker (n=30)

Table 4.1 shows the mean age for the IBT group to be 41.2. The mean age for the CBT group is 45.5. The overall study population shows there were more female participants (57%) than male participants (43%). Within the

instructor-based training method, however the female (61%) to male (39%) ratio was even greater. The computer-based training sessions were more comparable to the overall ratios with females representing slightly over half (54%), while the males represented slightly under half (46%) of the CBT study population.

Knowledge Transfer

H_0: There will be no statistically significant difference between participants who participate in traditional instructor-based classroom information security training and those who participate in computer-based information security training when comparing the results of standardized post-test quizzes.

H_1: Employees who participate in traditional instructor-based classroom information security training perform statistically significantly better on the standardized post-test quizzes than those who participate in computer-based information security training when comparing the results of post-test quizzes.

A one-way analysis of variance (ANOVA) and the F-ratio were used for comparing the independent means of the post-test quiz scores of the participants within the two training groups. As shown in Table 4.2, the mean of the post-test score for participants in Group 1 (IBT) was 9.69, while the mean for Group 2 (CBT) was 9.59.

Table 4.2: Means of Short-term Post-test Quiz Scores for IBT and CBT Groups

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
1	85	9.69	.535	.058	9.58	9.81
2	127	9.59	.770	.068	9.46	9.73
Total	212	9.63	.686	.047	9.54	9.72

Table 4.2.1: F-Ratio of Short-term Post-test Quiz Scores for IBT and CBT Groups

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	.546	1	.546	1.161	.282
Within Groups	98.756	210	.470		
Total	99.302	211			

There was no statistically significant difference between Group 1 and Group 2 in post-test quiz scores at the .05 level of significance. The F-ratio was equal to 1.16 with a significance level of .282. Because the level of significance (.282) was not less than the critical value of .05, the null hypothesis (which stated there is no statistically significant difference between the two groups) could not be rejected.

A one-way analysis of variance (ANOVA) and the F-ratio were used for comparing the independent means of the transfer of knowledge scores of the participants within the two training groups. As shown in Table 4.3, the mean for transfer of knowledge for participants in Group 1 (IBT) was 2.64, while the mean for Group 2 (CBT) was 1.87.

Table 4.3: Means of Transfer of Knowledge Scores for IBT and CBT Groups

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					Lower Bound	Upper Bound
1	85	2.64	1.143	.124	2.39	2.88
2	127	1.87	1.215	.108	1.66	2.09
Total	212	2.18	1.241	.085	2.01	2.35

Table 4.3.1: F-Ratio of Transfer of Knowledge Scores for IBT and CBT Groups

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	29.510	1	29.510	20.959	.000
Within Groups	295.678	210	1.408		
Total	325.189	211			

There was a statistically significant difference between Group 1 and Group 2 in the transfer of knowledge scores at the .000 level of significance. The F-ratio was equal to 20.959 with a significance level of .000, which is less than the critical value of .05. The IBT Group's level of knowledge transfer was statistically significantly higher than the CBT Group.

Analysis and Discussion

The results show that while both groups scored similarly on the post-test, when comparing the difference in increase of scores, IBT had a greater increase in post-test scores. The participants who participated in instructor-based information security training had a greater transfer of knowledge. The experimental design used in this study divided the bank employees into two groups, IBT (treatment) and CBT (control) groups. While both the treatment and control groups experienced a marked improvement over their pre-test scores, the IBT group experienced a statistically significantly greater increase in their post-test scores. Such findings suggest that organizations seeking to implement formal information security training programs should consider not just CBT modules but face-to-face traditional instructional methods as well.

The results of this study support Danziger's [7] study of perceived level of effectiveness between instructor-based and computer-based training. Danziger [7] found that participants who received IBT scored higher on post-test skills assessment compared to their CBT counterparts, due to the ability to receive one-on-one training with the instructor. Rehberg [24] also noted that within his study of CPR trainees, the IBT participants scored higher on job performance due to the hands on nature of the training material.

Knowledge Retention

H_0: There will be no statistically significant difference between participants who participate in traditional instructor-based classroom information security training and those who participate in computer-based information security training when comparing the results of long-term post-test quizzes (60 and 90 days).

H_1: Employees who participate in traditional instructor-based classroom information security training perform statistically significantly better on the 60 and 90 day post-test quizzes than those who participate in computer-based information security training when comparing the results of long-term post-test quizzes.

60 Day Post-test Results

A one-way analysis of variance (ANOVA) and the F-ratio were used for comparing the independent means of the 60-day post-test quiz scores of the participants within the two training groups. As shown in Table 4.4, the mean of the post-test score for participants in Group 1 (IBT) was 7.73, while the mean for Group 2 (CBT) was 8.30. The mean difference between the group scores is .57. There was a statistically significant difference between Group 1 (IBT) and Group 2 (CBT) in the 60 day post-test quiz scores.

Table 4.4: Means of 60-Day Post-test Quiz Scores for IBT and CBT Groups

					95% Confidence Interval for Mean	
	N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound
1	41	7.73	1.025	.160	7.41	8.06
2	46	8.30	1.133	.167	7.97	8.64
Total	87	8.03	1.115	.120	7.80	8.27

Table 4.4.1: F-Ratio of 60-Day Post-test Quiz Scores for IBT and CBT Groups

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	7.109	1	7.109	6.055	.016
Within Groups	99.788	85	1.174		
Total	106.897	86			

There was a statistically significant difference between Group 1 and Group 2 in the 60-day post-test quiz scores at the .016 level of significance. The 60-day post-test results for Group 2 (CBT) were statistically significantly higher than Group 1 (IBT). The F-ratio was equal to 6.05 with a significance level of .016. Because the level of significance (.016) was less than the critical value of .05, the null hypothesis (which stated there is no statistically significant difference between the two groups) was rejected.

90 Day Post-test

A one-way analysis of variance (ANOVA) and the F-ratio were used for comparing the independent means of the 90-day post-test quiz scores of the participants within the two training groups. As shown in Table 4.6, the mean of the post-test score for participants in Group 1 (IBT) was 7.97, while the mean for Group 2 (CBT) was 8.09. The mean difference between the group scores is .12. There was no statistically significant difference between Group 1 and Group 2 in post-test quiz scores.

Table 4.6: Means of the 90-Day Post-test Quiz Scores for IBT and CBT Groups

					95% Confidence Interval for Mean	
	N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound
1	33	7.97	1.045	.182	7.60	8.34
2	54	8.09	.807	.110	7.87	8.31
Total	87	8.05	.901	.097	7.85	8.24

Table 4.6.1: F-Ratio of 90-Day Post-test Quiz Scores for IBT and CBT Groups

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	.309	1	.309	.378	.540
Within Groups	69.507	85	.818		
Total	69.816	86			

There was no statistically significant difference between Group 1 and Group 2 in post-test quiz scores at the .05 level of significance. The F-ratio was equal to .378 with a significance level of .540. Because the level of significance (.540) was greater than the critical value of .05, the null hypothesis (which stated there is no statistically significant difference between the two groups) could not be rejected.

Analysis and Discussion

The results show that while both groups scored similarly on the short-term post-test (Table 4.3 and 4.3.1), there was a significant difference in the 60 day post-test scores. The CBT participants had statistically significantly higher 60 day post-test scores than the IBT participants. Kohen and Kipps' [17] seminal study of microeconomics and students' knowledge retention of course material also introduced the term knowledge "depreciation" (p.40). Kohen and Kipps [17] found that students' experienced a greater level of knowledge depreciation over a longer period of time, for example the three-month summer semester break, as opposed to a month-long winter recess. The researchers found in their study that knowledge depreciates as time increases.

In contrast to the 60-day post-test results, the 90-day post-test results indicate a leveling out of knowledge retention between the instructor-based group and the computer-based group. The results indicate that there is no difference in knowledge retention levels between the two groups at the 90-day time period. Similarly, as noted above in the 60-day post-test retention results, this finding would be important for organizations seeking to ensure that employees retain the training knowledge for the long-term. Both training groups (IBT and CBT) did not retain the training material for the extended time period, regardless of training delivery mode. The results also imply that in order for the training to have a lasting effect, an organization must repeatedly provide reminders of training material [3]. As the findings show, there was a negligible difference in the 90-day post-test scores regardless of training delivery mode. Organizations that are implementing formal information training programs should consider scheduling regular and consistent training throughout the year, beyond the 90-day time period.

While both the treatment and control groups experienced a decrease in scores from their short-term post-test scores, the IBT group experienced a statistically significantly greater decrease than their CBT counterparts. This finding would be important for organizations seeking to ensure that training programs not only increase transfer of knowledge, but also improve retention of training knowlede. While face-to-face training may provide an immediate increase in transfer of knowledge, it does not necessarily mean the material will be retained for an extended time period.

As Argyris and Schon [2] explain, in order for organizations to learn effectively, they must make the transition from working theory to theory in action, or theory in use. Organizations that are implementing training programs should consider scheduling regular, year-round and consistent training to ensure the training material is on the forefront of people's minds. In order to increase information security awareness, organizations must remind employees of the training material or they will not retain the knowledge or skills acquired [26]. The results of this study appear to support Reid's [25] longitudinal study of knowledge retention for computer-based training participants, in which the CBT group scored significantly higher on all content evaluation post-tests than other training groups, including IBT and no training.

CONCLUSION

The purpose of the research was to determine the effectiveness of ABC Bank's instructor-based and computer-based information security training programs. The effectiveness of the bank's IBT and CBT information security training program was measured by multiple variables including transfer of knowledge, retention of knowledge, and level of satisfaction.

The results of this study showed a statistically significant difference in the increase in pre-test to post-test scores, or transfer of knowledge scores between the IBT group and the CBT group. The IBT Group's level of knowledge transfer was higher than the CBT Group. The results of this study may be meaningful for an organization that is beginning to implement a corporate information security training program. This is especially true with the rapid adoption of online learning initiatives, web-based training systems, and the ubiquity of computer-based training programs [9]. Although computer-based training programs are becoming more common [11], the results of this study show that instructor-based training can be just as, if not more effective in raising the level of information security awareness. Minimally, these results support the need for organizations to further research and consider instructor-based training as a viable alternative to computer-based training programs.

There was a statistically significant difference between the IBT and CBT groups in the 60-day post-test quiz scores. The 60-day post-test results for the CBT Group were statistically significantly higher than their instructor-based counterparts. The results show that while both groups scored similarly on the short-term post-test, the computer-based training participants had statistically significantly higher 60 day post-test scores than their instructor-based employees. Not surprisingly, there was also a statistically significant difference between the two groups in the level of knowledge depreciation. That is, the IBT participants' knowledge depreciated at a higher rate than the CBT participants.

While both IBT and CBT participants experienced a decrease in scores from their short-term post-test scores, the IBT group experienced a statistically significantly greater decrease than their CBT counterparts for the 60-day post-test. The findings for this study at ABC Bank suggest that while face-to-face training may provide a higher, immediate increase in transfer of knowledge, it does not necessarily mean the material will be retained for an extended time period.

In direct contrast to these findings, it was noted that the 90-day post-test resulted in no significant difference between IBT and CBT test scores. After three months, all trainee participants reverted back to almost identical pre-test scores. This could be an interesting finding for the financial service industry. Many banks that implement information security training are often first attempting to meet compliance and regulatory standards or meeting an audit objective. And while it is important for banks to implement training, management has to take the next step and

ask what is going to be the long-term benefit of training? Organizations that spend the time and resources to implement formal information security training program should also make the effort to review the effects, or "results" of their programs to determine that time and resources spent actually result in a more secure environment.

The results of this study also imply that in order for the training to have a lasting effect, an organization must repeatedly provide reminders of training material. As the findings show, there was a negligible difference in the 90-day post-test scores regardless of mode of training delivery. Meaning after 90 days, everyone regressed back to pre-test levels of knowledge.

Knowledge gained through corporate training should be incorporated into the everyday routine and culture of the organization [31]. McIlwraith [20] suggests methods for building and retaining an information security conscious community could include: bulletin and message boards, wikis, newsletters, and other reminders to remind and reinforce information security training concepts. Organizations implementing formal information training programs should consider scheduling regular and consistent training throughout the year, beyond the 90-day time period. We recommend incremental and strategic information security training programs every quarter to ensure training material is not forgotten.

REFERENCES

1. Alliger, G. M., & Janak, E. A. (1989). Kirkpatrick's level of training criteria: Thirty years later. Personnel Psychology, 42(2), 331-342.
2. Argyris, C. & Schon, D. (1978). Organizational Learning: A theory of action perspective. Addison-Wesley.
3. Arthur, W., Bennett, W., Edens, P. L., & Bell, S. T. (2003). Effectiveness of training in organizations: A meta-analysis of design and evaluation features. Journal of Applied Psychology, 88.
4. Bhatti, R., Bertino, E. & Ghafoor, A. (2007). An integrated approach to federated identity and privilege management in open systems. Communications of the ACM, 50(2), 81-87.
5. Cox, J. (2002). Survey: Security remains job 1. Network World [Electronic Version]. Retrieved November 10, 2008, from http://www.networkworld.com/news/2002/0520nw500.html.
6. CSI 2007. (2007). 2007 CSI computer crime and security survey. Retrieved October 15, 2008 from http://www.gocsi.com.
7. Danziger, J. N. (2000). Enhancing end users' ICT skills in the new economy. Center for research on ICT and Organizations; University of California Irvine.
8. Greene, S. S. (2006). Security policies and procedures, principles and practices. New York: Pearson Prentice Hall.
9. Hwang, G. J., Wu, T. T., & Chen, Y. J. (2007). Ubiquitous computing technologies in education. Journal of Distance Education Technology, 5(4), 1-4.
10. Im, G. P. & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. The Database for Advances in Information Systems, 36(4), 68-79.
11. Jones, V. & Jo, J. H. (2004). Ubiquitous learning environment: An adaptive teaching system using ubiquitous technology. Proceedings of the 21st ASCILITE Conference, 468-474.
12. Jorgenson D.W. & Stiroh, K.J. (1995). Computers and growth. Economics of Innovation and New Technology, 3(3-4), 249-83.
13. Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. International Journal of Electronic Commerce, 12(1), 69-91.
14. Kavanagh, J. (2004). Human failings can compromise the best IT security configuration. Computer Weekly, February 2004, 48.
15. Kim, E. B. (2005). Information security awareness status of full time employees. The Business Review, Cambridge, 3(2), 219-226.
16. Kirkpatrick, D. L. (1967). Evaluation of training. In Craig R. L., Bittel L. R. (Eds.). Training and Development Handbook (pp. 87-112). New York: McGraw-Hill.
17. Kohen, A.I. and Kipps, P.H. (1979). Factors determining student retention of economic knowledge after completing the principles-of-microeconomics course. Journal of Economic Education, 10(2), 38-48.

18. Knowles, M. S. (1970). The modern practice of adult education: Andragogy versus pedagogy. Englewood Cliffs, Cambridge: Prentice Hall.
19. Knowles, M. S. (1984). Andragogy in action. San Francisco, CA: Jossey-Bass.
20. McIlwraith, A. (2006). Information security and employee behaviour: How to reduce risk through employee education, training, and awareness. Burlington, VT: Gower Publishing Company.
21. Pollitt, D. (2005). Energis trains employees and customers in IT security. Human Resource Management International Digest, 13(2), 25-28.
22. Porter, M. E. & Millar, V. E. (1985). How information gives you competitive advantage. Harvard Business Review, July-August 1985, 149-174.
23. Price Waterhouse Coopers. (2008). Safeguarding the new currency of business: Findings from the 2008 global state of information security study. Retrieved from http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/Safeguarding_the_new_currency.pdf.
24. Rehberg, R. R. (2003). Classroom versus computer-based CPR training: A comparison of the effectiveness of two instructional methods. Ph.D. dissertation, Touro University International University, 2003, (3077390).
25. Reid, D. (2001). Knowledge retention in computer-based training. M.A. thesis, University of Calgary, 2001, (0-612-65050-2).
26. Siponen, M. T. (2000). A conceptual foundation for organization information security awareness. Information Management & Computer Security, 8(1), 31-41.
27. Sullivan, R. J. (2000). How has the adoption of internet banking affected performance and risk in banks? Financial Industry Perspectives, 2000, 1-16.
28. Sullivan, B. (2004). Your evil twin: Behind the identity theft epidemic. Hoboken, New Jersey: John Wiley & Sons.
29. Swartz, N. (2008). Record data breaches in 2008. Information Management Journal, 42(6), 20.
30. Whitman, M. & Mattord, H. (2003). Principles of information security. Boston, MA: Thomson Course Technology.
31. Zolingen, S. V., Streumer, J., & Stooker, M. (2001). Problems in knowledge management: A case study of a knowledge-intensive company. International Journal of Training and Development, 5(3), 168-184.