Issues in Information Systems
Volume 17, Issue IV, pp. 197-207, 2016

HOW LONG DO EMPLOYEES REMEMBER INFORMATION SECURITY TRAINING PROGRAMS? A STUDY OF KNOWLEDGE ACQUISITION AND RETENTION

Philip Kim, Walsh University, pkim@walsh.edu
Joseph V. Homan, Monterey Technologies, Inc., jhoman@mti-inc.com
Richard L. Metzer, Robert Morris University, rlmst26@mail.rmu.edu

ABSTRACT

Organizations mitigate information security risk by providing relevant and timely training for end users. While training budgets have increased in recent years, few organizations have taken the next step to measure how effective these programs are in changing behavior. An antecedent to behavioral change is increasing knowledge. This study explores the effectiveness of an information security training program by measuring the differences in pre and post-test results to determine levels of knowledge acquisition and knowledge retention. The results of this study showed a statistically significant difference in the increase in pre to post-test scores within the participant groups. The instructor-led group's level of knowledge acquisition was higher than the computer-based training group. The results of this study may be meaningful for an organization that is in the beginning stages of implementing a corporate information security training program.

Keywords: Information Security Training, Organizational Development, CBT, IBT, Knowledge Retention

INTRODUCTION

Organizations that seek to enhance their information security posture must raise the level of awareness of information security threats and risks among the end-users and other non-IT related departments (Rotvold, 2008; Skovira, 2007). The role of securing corporate information systems and proprietary data has traditionally fallen primarily on the companies' IT departments, but there is a growing movement to make information security an enterprise-wide endeavor (Lohmyer, McCrory, & Pogreb, 2002). An effective information security training and awareness program is a critical component of protecting an organization's information assets (Peltier, 2001).

Financial institutions are increasingly finding difficulty defending against information security risks and threats (Price, 2014). Financial institutions are often the number one target for information thieves and due to limited technical and human resources many banks are not prepared to protect against information security threats (Urrico, 2016). There has been accelerated growth in spending within professional development and corporate training as employers are expanding and developing their talent base (Bersin, 2014). According the 2014 State of the Industry Report, with over $160 billion spent of corporate training (ATD, 2014), employee education and learning continue to be key priorities for many organizations. While many companies have invested numerous resources in implementing information security training and awareness programs, the problem is that few have explored deeper to examine the effectiveness of these training programs.

Modes of Training Delivery

While corporate training budgets have increased, so have the options for mode of delivery. The advancement of online technologies and learning environments have progressed corporate training from traditional instructor-led training to e-learning modules, which can include anything from low or no cost web courses, online videos, and MOOCs (massive, open, online courses) to higher cost custom web-based training solutions (Clarke, 2013).

The purpose of the study was to examine the effectiveness of an information security awareness program within a mid-sized publicly traded 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, and the ability of the trainee to retain the knowledge of information security awareness standards. 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 of effectiveness, or differing levels of knowledge acquisition and knowledge retention of the information security awareness standards.

Research Questions

To examine the effectiveness of information security training, the goal of this research was to answer the following questions:

RQ 1: In what ways could different modes of information security training impact the level of participants' awareness of information security standards?

RQ 2: In what ways could different modes of information security training impact the participants' ability to retain the knowledge of information security standards?

A research study that measures the effectiveness of information security training will be relevant to any organization looking to enhance its information security control environment. Specifically the results of this study will be useful for organizations that are seeking to determine the mode of delivery best suited for its organizational development and training needs.

LITERATURE REVIEW

Adult Learning Theory

Malcolm Knowles' (1970) Andragogy theory of adult learning is important to this study because it focuses on the adult learning and educational experience. Knowles (1970) argues that the adult learning experience is dissimilar to the child learning experience, therefore should be studied in contrast to existing child-based learning research. The four primary principles of adult learning according to Knowles are 1) adults need to be involved with the planning of their education, 2) the ability for adults to incorporate previous life experiences into training is an important part of the learning process, 3) adults have greater incentive to learn when the material relates directly to their current job, and 4) adults learn best through problem-solving scenarios. The Andragogy model of learning was utilized 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.

Lerner (1997) argues that the student are more likely to learn if there is increased involvement or interaction with the course material. When the learner is able to control or construct his or her learning material, there is greater understanding and depth to the knowledge acquired. Students learn more effectively when they are able to actively interact with the material being taught, as opposed to passively reading the corporate policy or signing an acceptable usage statement.

Argyris and Schon's (1978) Organizational Learning Theory provide another framework to measure how employees within an organization learn. Employees of an organization learn in different stages or phases. After employees learn the training material, they 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 (Argyris & Schon, 1978).

Byres and Lowe (2004) conducted a study that reviewed historical data on information security breaches between 1982 and 2003 and found that through the first 18 years of the data, the threat sources for information security breaches were split evenly between internal and external. The data from 2000 through 2003 shows a significant shift

to about 70% of all security breaches originate from external sources. Byres and Lowe (2004) explain "[t]he increasing interconnection of critical systems has created interdependencies," (p.3) which can lead companies to not only share their data, but also share an increased exposure to external Internet attacks and threats such as viruses and worms. However, while internal data breaches are less common than external data breaches, they are far more damaging to data security because the internal employee already has access to confidential data and is more likely to be trusted (Garfinkel, Gopel, & Goes, 2002).

Computer-Based Training and Instructor-Based Training

Traditionally, the primary method of training for most organizations has been the classroom, instructor-led, or instructor-based training (IBT) setting. The IBT method primarily consists of an instructor or instructors training employees through the use of seminar-style lecture or discussion, which may or may not include audio and visual aids such as the use of a personal computers (PC), projection systems, and/or presentation slides.

IBT can be conducted in a one-on-one or in a group setting. The one-on-one setting is beneficial for individual learner because it allows the instructor to develop or modify the training material that can address specific training needs of the single trainee. However, IBT is more often utilized in a group, classroom setting, facilitating group interaction, discussion, and group learning activities (Feather, 1999). Students learn more in a group setting because of working together and engaging in group problem solving. Another benefit of IBT is the giving and receiving immediate instructor feedback and encouraging peer interaction and feedback (Bostrom, Olfman, & Sein, 1990).

A significant benefit of computer-based training is the lower cost of delivery. While the initial cost of purchasing a CBT module or software program may be higher than IBT, the long-term benefits, re-usability, and delivery methods are lower (Cassavaugh, 2007). Harrington and Walker (2003) argue another benefit of CBT is that it works well with adults because the trainee feels that he is in control of the training program. CBT allows for the trainee to complete the training program at their own pace, within a location of their choosing, supports flexible schedules, and is available at any time that is convenient for the trainee.

Some organizations and scholars have taken the next step to research and compare the differences in the overall impact of the two training modes (CBT and IBT). The studies that compare the differences between CBT and IBT have defined the effectiveness of training by measuring the resulting increase in transfer of skills or increase in job performance. A study by Rehberg (2003) measured the impact of computer-based training and instructor-based training on the transfer of cardiopulmonary resuscitation (CPR) skills, and found that CBT training was just as effective as IBT training in terms of transfer of skills as measured by a post-training assessment, however the study found that the instructor-based training led to greater job performance due to the "hands on" nature of the CPR training. Rehberg (2003) explains that IBT training may have been more effective because it allowed the students to better understand the nuances of physically administering CPR on the mannequin.

Wendt (2000) conducted a study that measured the impact of training and the transfer of knowledge based on two types of training modes, instructor-led delivery and computer-based delivery. The results indicate that CBT was just as effective if not more effective in the students' ability to learn fundamental technology-related basics. The results of the posttest mean scores in Wendt's (2000) study showed that CBT participants scored slightly higher than their instructor-led counterparts. The findings from this study were significant, because the organization was in the process of implementing an enterprise-wide, global distance learning module.

Danziger (2000) conducted a study of training effectiveness at a multi-national technology company. The technology company administered a web survey to its employees, and the survey results were gathered from a study population of 398 employees. Danziger's (2000) study collected data on the end-user's experience with different training modes, including IBT and CBT, and their perceived level of effectiveness of the company's technology training programs. The findings showed that trainees who received more instructor-based or one-on-one instruction scored "[t]he highest mean of effectiveness of training is reported by end users who experienced [instructor-based] training" (Danziger, 2000, p.10). In contrast, the CBT mode was assessed to be least effective. The lower scores for the CBT mode may be attributed to the employees' lack of acceptance towards non-personal training methods such as CBT, video conferencing, and e-learning. Only 10% of the study population reported participating in CBT.

Further studies have researched training effectiveness by measuring an increase in job performance (Gustafson, 1977; Bates, Holton, Seyler, & Carvalho, 2000) and found varying results within various industries including how to improve the process of coding application software (Holmes, 1988), database concepts (Mollick, 2002), and increased physical responses to visual media (Cassavaugh, 2007).

Knowledge Retention

Knowledge retention is an important component of this study. It has been argued that information security training is necessary for corporations to keep their data secure (Snyder, 2006; Young, 2006), but how do employees remember the training materials taught in the information security training and awareness programs? For the purposes of my study, knowledge retention will be defined as the trainee's ability to remember the acquired knowledge of the material presented within the ISTA programs, over a set period of time.

Reid (2001) conducted a longitudinal study that measured the level of knowledge retention of employees who experienced three different types of computer-based training, CBT with no review activities, CBT with user-generated review activities, and CBT with program-generated review activities. Knowledge retention was measured by administering content evaluation post-tests upon completion of the training. The post-tests were administered immediately upon training intervention, and then again after 30 days and 60 days upon completion of the CBT training Reid (2001) found that the group that experienced CBT with program-generated review activities scored significantly higher on all content evaluation post-tests than the other two groups.

Kohen and Kipps (1979) conducted a study to determine what factors affected the students' ability to retain knowledge of course material upon completion of a Principles of Microeconomics course at James Madison University. An interesting result of the Kohen and Kipps (1979) study is the concept of knowledge loss or information "depreciation" (p.40). Knowledge depreciation is the rate of knowledge that decreases as a function of time and other factors such as student ability and grade point average. Knowledge depreciates as time increases. For the students in this study, micro-economic knowledge tended to depreciate at approximately 20% per year. Similarly to the Kohen and Kipps (1979) study, this research study will seek to determine if and what information the students have been able to retain of the training course material and to what depth of understanding after a specified time interval. This study will also explore the differences and possible relationships between the two modes of training delivery, various demographic data, and the ability to retain knowledge of the information security training program.

RESEARCH METHODOLOGY

A quantitative design was used for this study in order to gather numerical data to measure the effectiveness of an information security awareness program. For the purpose of this study, effectiveness of the information security awareness program has been operationalized as an increase in participants' knowledge of information security standards and the ability of the participant to retain the newly acquired knowledge. These levels of knowledge acquisition and retention were determined by post-training assessments. The information security awareness program within this study included two modes of information security training which contained identical training material. The two modes included a computer-based training (CBT) module and an instructor-based training (IBT) module.

Prior to the training sessions, a pre-test knowledge quiz was administered to determine participants' current level of information security knowledge prior to training. After the training session was been completed, 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 a change 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.

As noted previously, there were two post-test examinations. 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 periods of time.

Participants

The information security awareness program is mandatory for all full-time employees while part-time and temporary employees are exempt from the mandatory training requirements. The population of this study was 204 full-time employees of the organization. There were 85 employees who chose the instructor-based training sessions and 119 employees who chose computer-based training sessions.

Instrumentation

The computer-based training module has been developed by BVS Training Solutions Incorporated (BVS). BVS is a leading training and development company that specializes in providing training solutions for over 1,000 financial institutions. BVS has over 30 years' experience developing CBT for banks and credit unions in such diverse areas as: regulatory compliance, security, customer service and sales. The CBT module that was utilized for this study is a BVS training course entitled *Information Security Basics Course 20XX*. The BVS CBT modules were provided on ABC Bank's workstations, through the corporate local and wide area network.

The topics of the training cover a broad range of information security awareness including but not limited to, management's role in securing information, the employee's role in information security, confidentiality of corporate data, the physical and logical security procedures in place, and finally social engineering. Social engineering is the act of using social interactions to obtain unauthorized confidential or sensitive information (Granger, 2001).

RESULTS

A total of 212 employees participated in either the instructor-based training (IBT) session (code = 1) or the computer-based training (CBT) training session (code = 2). As Figure 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 demographic characteristics such as age, gender, job title, and previous participation in the BVS information security training session were collected via demographic survey.

Figure 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:	40.1%	59.9%	100.0%
Mean Age:	41.2	45.5	43.8
Gender:			
Male:	38.8%	45.7%	42.9%
Female:	61.2%	54.3%	57.1%
Modal Job Title:	Branch Manager (n=15)	Personal Banker (n=17)	Personal Banker (n=30)

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 Acquisition

RQ1: In what ways could different modes of information security training impact the level of participants' awareness of information security standards? Is there a statistically significant difference on short-term posttest scores?

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

Table 1. F-Ratio of Short-term Posttest Quiz Scores for IBT and CBT Groups

					95% Confidence Interval for Mean	
	N	Mean	Std. Deviation	Std. Error	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

	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 (IBT) and Group 2 (CBT) in posttest 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.

Level of Knowledge Acquisition Comparing Between IBT and CBT

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 (instructor-based training) was 2.64, while the mean for Group 2 (computer-based training) was 1.87.

Table 2. F-Ratio of Knowledge Acquisition Scores for IBT and CBT Groups

					95% Confidence Interval for Mean	
	N	Mean	Std. Deviation	Std. Error	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

	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 is 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 acquisition was statistically significantly higher than the CBT Group.

The results show that while both groups scored similarly on the posttest, when comparing the difference in increase of scores, the instructor-based training had a greater increase in posttest scores. The participants who participated in instructor-based information security training had a greater transfer of knowledge. The results of this study support Danziger's (2000) study of perceived level of effectiveness between instructor-based and computer-based training. Danziger (2000) found that participants who received instructor-based training scored higher on posttest skills assessment compared to their computer-based counterparts, due to the ability to receive one-on-one training with the instructor. Rehberg (2003) also noted that within his study of CPR trainees, the instructor-based training participants scored higher on job performance due to the hands on nature of the training material.

Knowledge Retention

RQ2: In what ways could different modes of information security training impact the participants' ability to retain the knowledge of information security standards? Is there a statistically significant difference in the long-term posttest scores?

60 Day Posttest Results

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

Table 3. F-Ratio of 60-Day Posttest 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

	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 is a statistically significant difference between Group 1 and Group 2 in the 60-day posttest quiz scores at the .016 level of significance. The 60-day posttest 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.

The results show that while both groups scored similarly on the short-term posttest (Table 3), there was a difference in the 60 day posttest scores. The computer-based training participants had statistically significantly higher 60 day posttest scores than their instructor-based employees. The results of this study appear to align with Kohen and Kipps' (1979) seminal study of knowledge depreciation, however this study included computer-based training as an independent variable.

90 Day Posttest

A one-way analysis of variance (ANOVA) and the F-ratio were used for comparing the independent means of the 90-day posttest quiz scores of the participants within the two training groups. As shown in Table 4.6, the mean of the posttest score for participants in Group 1 (instructor-based training) was 7.97, while the mean for Group 2

(computer-based training) 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 posttest quiz scores.

Table 4. F-Ratio of 90-Day Posttest Quiz Scores for IBT and CBT Groups

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean	
					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

	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 posttest 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.

CONCLUSION

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 acquisition was higher than the CBT Group. The results of this study may be meaningful for an organization that is in the beginning stages of implementing 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 (Bartley & Golek, 2004). Although computer-based training programs are becoming more common, 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.

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. Van Zolingen, Streumer, and Stooker (2001) argue that knowledge gained through corporate training should be incorporate into the everyday routine and culture of the organization. Organizations that are implementing formal information training programs should consider scheduling regular and consistent training throughout the year, beyond the 90-day time period.

The results of this study show that neither computer-based instruction nor instructor-based instruction significantly affected trainees' level of knowledge acquisition and knowledge retention. Thus, it could be concluded that computer-based instruction and instructor-based instruction are similar in terms of their efficacy in the transfer of knowledge and long-term retention of training knowledge.

There should be a consideration for scheduling regular, year-round and consistent training to ensure the training material is not forgotten. McIlwraith (2006) 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.

REFERENCES

Argyris, C. & Schon, D. (1978). *Organizational Learning: A theory of action perspective.* Addison-Wesley.

ATD. (2014). 2014 State of the industry report: spending on employee training remains a priority. Association for Talent Development. Retrieved from: https://www.td.org/Publications/Magazines/TD/TD-Archive/2014/11/2014-State-of-the-Industry-Report-Spending-on-Employee-Training-Remains-a-Priority.

Bartley, S. J., & Golek, J. H. (2004). Evaluating the Cost Effectiveness of Online and Face-to-Face Instruction. *Educational Technology & Society*, *7*(4), 167-17.

Bates R. A., Holton E.F., Seyler D.L., & Carvalho M.A. (2000). The role of interpersonal factors in the application of computer-based training in an industrial setting. *Human Resource Development International*, *3*(11), 19-42.

Bersin, J. (2014). Spending on corporate training soars: employee capabilities now a priority. Forbes. Retrieved from: http://www.forbes.com/sites/joshbersin/2014/02/04/the-recovery-arrives-corporate-training-spend-skyrockets/#1faa380c4ab7.

Bostrom, R. P., Olfman, L., & Sein, M. K. (1990). The importance of learning style in end-user training. *MIS Quarterly, 14*(1), 101-119.

Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. *In Proceedings of the VDE Kongress, 116*, 213-218.

Clarke, T. (2013). The advance of the MOOCs (massive open online courses). The impending globalisation of business education? *Education & Training*, *55*(4/5), 403-413.

Danziger, J.N. (2000). Enhancing end users' ICT skills in the new economy. *Center for research on ICT and Organizations*; University of California Irvine.

Feather, S.R. (1999). Impact of group support systems on collaborative learning groups' stages of development. *Information Technology, Learning, and Performance Journal, 17*(2), 23-34

Garfinkel, R., Gopal, R., & Goes, P. (2002). Privacy protection of binary confidential data against Deterministic stochastic, and insider threat. *Management Science 2002, 48*(6), 749-764.

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus, December, 18*.

Gustafson, H.W. (1977). Job performance evaluation as a tool to evaluate training. *Improving Human Performance Quarterly, 5*, 133-152.

Harrington, S., & Walker, B. (2003). Is computer-based instruction an effective way to present fire safety training to long-term care staff? *Journal for Nurses in Staff Development, 19*(3), 147-154.

Holmes, S.H. (1988). A comparative assessment of computer-based training (CBT) and the traditional industry lecture methodology upon job performance in application software training. Ed.D. dissertation, Pepperdine University, 1988, (8918738).

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.

Knowles, M.S. (1970). *The modern practice of adult education: Andragogy versus pedagogy.* Englewood Cliffs, Cambridge: Prentice Hall.

Lerner, M. (1997). The current state of technology and education: How computers are used in K-12 and brown university classrooms (On-line). Retrieved from: http://www.netspace.org/-mrl/handbook/int_ed.html.

Lohmyer, D.F., McCrory, J., & Pogreb, S. (2002). Managing information security. *The McKinsey Quarterly 2002 Special Edition: Risk and Resilience*, 12-15.

McIlwraith, A. (2006). Information security and employee behaviour: How to reduce risk through employee education, training, and awareness. Burlington, VT: Gower Publishing Company.

Mollick, K. (2002). The effects of computer-based training on rural college students' achievement in learning elementary database concepts. Ed.D. dissertation, Texas A&M University-Commerce, 2002, 3110312.

Peltier, T.R. (2001). *Information security risk analysis.* Boca Raton, Florida: CRC Press LLC.

Price, L. (2014). Financial institutions are a top target for malware attacks. *Security Intelligence*. Retrieved from: https://securityintelligence.com/financial-institutions-top-malware-attacks-target.

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).

Reid, D. (2001). Knowledge retention in computer-based training. M.A. thesis, University of Calgary, 2001, (0-612-65050-2).

Rotvold, G. (2008). How to create a security culture in your organization. *The Information Management Journal,* November/December 2008, *42*(6), 32-38.

Skovira, R. J. (2007). Framing the corporate security problem: The ecology of security. *Issues in Informing Science and Information Technology*, *4*, 45-52.

Snyder, J. (2006). Not investing in training. *Network World. 23*(33), 54.

Urrico, R. (2016). Financial institutions among top mobile hacker targets. *Credit Union Times*. Retrieved from:http://www.cutimes.com/2016/01/12/financial-institutions-among-top-mobile-hacker-tar?slreturn=1463750632.

Van Zolingen, S. J., Streumer, J. N., & 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.

Wendt, J. (2000). The impact of classroom instruction versus computer-based instruction on participant learning of technical Information. Ph.D. dissertation, Capella University, 2000, 3002457.

Young, T. (2006). Implementing a knowledge retention strategy: A step-by-step process to combat organization knowledge loss. *KM Review*, *9*(5), 28-33.