December 2006

Information System Security: Self-Efficacy and Implementation Effectiveness

Daniel Phelps
Florida State University

John Gathegi
Florida State University

Information System Security: Self-Efficacy and Implementation Effectiveness

Daniel C. Phelps
Florida State University
dphelps@ci.fsu.edu

John N. Gathegi
Florida State University
jgathegi@ci.fsu.edu

ABSTRACT

This study proposed a model for measuring information system security self-efficacy and examined the relationship between the educational preparation of librarian IT professionals and the effectiveness of their information system security implementation. It differentiated education based on whether or not the participant had received other, formal information technology training. It examined the relationship between information technology training and information system security effectiveness through the intervening variables of information system security experience, information system security self-efficacy, information system security task initiation, and information system security task persistence.

The study found that systems librarians with prior information technology training were more effective at implementing information system security than those without. Although the study failed to offer support for the model as a whole, significant relationships were found between prior information technology training, information system security self-efficacy, and information system security implementation effectiveness.

Keywords

Information System Security, Information Security Management, Information System Management, Security Education

INTRODUCTION

It has often been recognized that effective information security programs consist of appropriately managed technical controls, policies, and human behavior. Problems in any of these areas potentially lead to an ineffective information security program (Wade, J., 2004; Kabay, M.E., 2005). The recognition of human behavior's influence in information system security is important, at both the user and information technology (IT) professional level. A recent analysis of end user security behaviors demonstrated that password "hygiene," such as frequent changes to one's password, was generally poor, but improved with appropriate training, awareness, monitoring, and motivation (Stanton, et. al., 2005). Additionally, a recent survey completed by the Computing Technology Industry Association (2006) found that human error was responsible for approximately 60% of information system security breaches in 2005, but only 29% of the study participants required security training for their employees and only 36% even offered end-user security training. Compounding the problem, security awareness and training is often the first area cut when funding in information security is reduced (Schultz, E., 2004).

While both users and IT professionals require appropriate training in information system security concepts, it is generally the IT professional that can instantiate controls to assist the user with appropriate security behaviors, such as password choice and hygiene, and is also responsible for educating management about appropriate policies to help in creating and maintaining a secure environment. While in larger organizations, one may expect that IT professionals have both an appropriate educational background and experience, this is often not the case in smaller organizations. In the private sector, a recent examination of information systems security issues and decisions for small businesses found that many small businesses lacked the ability to make appropriate information system security choices (Gupta and Hammond, 2005). In the public sector, systems librarians are in a similar position. Systems librarians are a group of professionals typically brought into a position of responsibility for IT systems with limited IT backgrounds and almost no education or training in IT security (Newby, G., 2000; Xu, H. & Chen, H. L., 1999; Xu, H. & Chen, H. L., 2000a; Xu, H. & Chen, H. L., 2000b). Systems librarians were chosen as the population for this study specifically because they are in the unique position of being in an IT professional role, with increasing institutional demands and recognition of the criticality of IT to their organization's mission, but many have not received specific training to be IT professionals. Since many small businesses may find themselves in a similar situation, the results may be more broadly applicable.

LITERATURE REVIEW

Research investigating computer use and behaviors has often utilized the construct of self-efficacy, derived from Bandura's Social Cognitive Theory. Self-efficacy, or the belief that an individual holds in their ability to accomplish a given task, exists in a "triadic reciprocality" of influence that includes environmental factors, behavior, and personal factors (Bandura, A., 1986). Perceptions of self-efficacy have been found to influence what behaviors individuals undertake (Bandura, A., 1977; Betz, N. E. & Hackett, G., 1981), their task persistence (Barling, J. & Beatie, R., 1983; Brown, I. & Inouye, D. K., 1978), their emotional responses (Bandura, A., 1977; Stumpf, S. A., Brief, A. P., & Hartman, K., 1987), and their level of attainment (Barling, J. & Beatie, R., 1983; Collins, J. L., 1982; Locke, E. A., Frederick, E., Lee, C., & Bobko, P., 1984; Schunk, D. H., 1981; Wood, R. & Bandura, A., 1989). Social Cognitive Theory posits that individuals with high levels of domain and task specific self-efficacy tend to be more willing to undertake domain related tasks, be more persistent in the face of related obstacles, and ultimately have higher levels of attainment in the domain and with the tasks than individuals with lower levels of domain and task self-efficacy.

Bandura (1986, p.391) defines self-efficacy as "People's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances. It is concerned not with the skills one has but with judgments of what one can do with whatever skills one possesses," and suggests that self-efficacy is developed through four main sources of influence: mastery experiences, vicarious experiences provided by social models, social persuasion, and somatic and emotional states (Bandura, A., 1994). The strongest determinant of self-efficacy is mastery experiences. Individuals that have had previous task specific success will have a robust belief in their ability to perform the same or similar task again. Failure, however, tends to undermine an individual's sense of task specific self-efficacy, particularly if the failure occurs early in the individual's task exposure, before a sense of task specific efficacy is developed.

Although not as strong an influence as mastery experiences, vicarious experiences through social models promotes self-efficacy development. Bandura (1994) states, "Seeing people similar to oneself succeed by sustained effort raises observers' beliefs that they too possess the capabilities…to succeed. By the same token, observing others fail despite high effort lowers observers' judgments of their own efficacy and undermines their efforts" (p. 75). The degree to which vicarious experiences impact self-efficacy is highly influenced by the perception of similarity between the individual and model, with models perceived as very different from the individual having much less impact on individual self-efficacy. Training that models behavior has been shown to directly affect both self-efficacy and post training performance.

If information system security awareness training is cut, or if an IT professional has not received appropriate information system security exposure in their education and training, then Social Cognitive Theory predicts that this will affect their sense of information systems security self-efficacy, which in turn will affect their willingness to undertake information system security related tasks and their persistence in the task if they were to encounter difficulties establishing, configuring, or maintaining information system security. This ultimately will be reflected in the effectiveness of the information system security implementation.

The importance of IT to libraries is demonstrated by their increasing expenditures for electronic resources, both for intellectual content, such as online access to commercial databases, and for infrastructure, including both numbers of terminals and bandwidth (Young, M., Kyrillidou, M., & Blixrud, J., 2002). Much professional literature has been devoted to discussing how to properly manage the security of this infrastructure, discussing types of attacks and security problems (Fore, J. A., 1997; Koga, J. S., 1990), how to respond to attacks (German, G., 1997; Muir, S. P., 1997; Rosaschi, J., 1997), how to setup more secure terminals (Biever, E. J., 1997; Brakel, G., 1997; Breeding, M., 1997; Garrison, W. V. & McClellan, G. A., 1997; Lynch, C., 1997; Marmion, D., 1997) and how to understand and manage security risk (Brandt, D. S., 2003; Robertson, G., 2003).

The literature related to Social Cognitive Theory and computer use demonstrates that self-efficacy, possibly mediated by attitude, is a strong predictor of computer related performance (Multon, K. D., Brown, S. D., & Lent, R. W., 1991; Wang, A. Y. & Newlin, M. H., 2002). The studies have found consistent support for the relationship predicted by Social Cognitive Theory and specifically have found that individuals with higher levels of self-efficacy exert more effort and persist longer at specific tasks than do less efficacious individuals. Self-efficacy, in turn, is developed primarily through direct, mastery experience, such as found in 'hands-on' information technology training. Accordingly, the following hypotheses are given:

Hypothesis 1: Systems librarians with information technology training will be more effective at implementing information system security than those without.

Hypothesis 2a: Training influences self-efficacy moderated by direct and indirect experience.

Hypothesis 2b: Self-efficacy influences effectiveness moderated by task initiation and task persistence.

SAMPLE AND METHODOLOGY

The population for this study consisted of systems librarians working at any of the 195 public and academic libraries in the state of Florida. Since the population was small, the entire population was included. A questionnaire to assess the relationship between IT specific training, information system security self-efficacy, and information system security implementation effectiveness was developed, pre-tested, and pilot tested with both research experts and a similar population of systems librarians not included in the study. The content domains were established based on a thorough review of the literature and derived from the constructs of Social Cognitive Theory. The first question asked the respondents if they had had any specific information technology training beyond what was offered in their professional education and was coded as a yes or no. Experience, both direct and indirect, in information system security was measured using Likert scale responses ranging from none to extensive. Persistence and task initiation were both predicted by theory to be significantly influenced by self-efficacy. Persistence was measured by presenting a scenario of having difficulty establishing or maintaining information system security, and provided a series of possible actions the subject could do in order to solve the problem. Task initiation was measured by a Likert scale question asking the respondent to indicate the number of hours per week that are dedicated to information system security work. The central construct, information system security self-efficacy, was measured by presenting a series of related tasks of varying difficulty, with the subject responding with a value from 0 to 100, with 0 indicating no confidence in their ability to accomplish the task, and a response greater than 0 indicating the strength of their confidence. To assist with validity, these items were derived from a series of relevant security tasks published by the Computer Emergency Response Team (CERT) at Carnegie Mellon University. Information system security implementation effectiveness was measured by 40 questions derived from ISO17799/BS7799.

After development and testing of the instrument, a three step procedure for the administration of the questionnaire was followed as suggested by Creswell (1994). The survey instrument was initially mailed to the 195 libraries identified as either public or academic by the state Division of Library and Information Services in early August of 2004. The packet contained a cover letter explaining the purpose of the study and a five page questionnaire. In addition, instructions were provided for respondents that preferred to complete the questionnaire online. Two weeks after the first mailing, a second, postcard mailing was sent to the entire population, thanking the individuals that had completed the survey, and encouraging participation by those who had yet to complete it. Two weeks later, a third mailing consisting of a letter and instructions for web completion of the instrument was sent. A final postcard mailing was sent one week later. 56 useable instruments were completed, providing a response rate of approximately 29%. Assessment of non-response bias was examined utilizing extrapolation methods, based on the assumption that "subjects who respond less readily are more like non-respondents" (Armstrong and Overton, 1977, p. 397). For this study, 12 instruments were returned several weeks later than the majority of respondents and were utilized as a surrogate for non-respondents. The differences in the means of the continuous research variables were compared. Results of an independent t-test comparison showed no significant difference in means between the normal respondents and the late respondents ($p<.05$). The item consistency reliability was measured using Chronbach's alpha, which was found to be acceptable at 0.9423. Three weeks after the last instrument was returned, the researcher solicited the respondents to retake the survey. Of the 56 usable, initial responses, 13 respondents completed the survey a second time. Independent t-tests were performed on each continuous variable of interest. The analysis of the test/re-test results showed no statistically significant differences between administrations ($p<.05$). Since the researcher was the sole administrator of the instrument, intercoder reliability was not an issue. Intracoder reliability was controlled for the paper version by software mechanisms that required valid responses for each question item when entering them for analysis.

RESULTS

Hypothesis 1

Discriminating the subjects based on having received formal information technology training provides two groups, those with formal information technology training (25 respondents) and those without (31 respondents). A comparison of the mean scores on information system security effectiveness and self-efficacy was examined (Table 1). A t-test comparison of means was performed, with the results indicating a statistically significant difference in means ($p<.05$), supporting the first hypothesis.

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Security Effectiveness	Equal variances assumed	2.572	.115	2.290	54	.026	6.7368	2.94157	.83927	12.63428
Security Self-Efficacy	Equal variances assumed	1.603	.211	-4.577	54	.000	-649.6439	141.92416	-934.19	-365.103

Table 1: Comparison of the Mean Scores on Information System Security Effectiveness Based on I.T. Training

Hypotheses 2a and 2b

Table 2 presents the means, standard deviations, and correlations among the study variables. A few patterns within the correlations are worth noting. The discriminant validity for the variables is relatively poor, with several variables correlating extremely highly with others. This is not unexpected, however, given that Social Cognitive Theory predicts a common relationship between four of the variables mediated through self-efficacy. With the exception of the relationship between direct and indirect experience (CI=20.32), the condition indexes were less than 15, indicating an acceptable tolerance for collinearity (SPSS, i., 1999).

	Mean	SD	1	2	3	4	5	6
IT Training	.45	.50						
Direct Security Experience	3.04	1.28	.36(**)					
Indirect Security Experience	3.16	1.08	.37(**)	.86(**)				
Hours/Week Security Tasks	2.50	1.90	.31(**)	.63(**)	.64(**)			
Security Persistence	3.41	1.86	.27(*)	.57(**)	.42(**)	.36(**)		
Implementation Effectiveness	58.09	11.36	-.30(*)	-.36(**)	-.41(**)	-.32(**)	-.029	
Security Self-Efficacy	1137.54	616.35	.54(**)	.74(**)	.68(**)	.61(**)	.47(**)	-.50(**)

Table 2: Correlations between Research Variables

Note. Values associated with dichotomous variables are Spearman's ρ, all other are Pearson's *r*. IT Training coded No=0, Yes=1. N=56.

* Correlation is significant at the 0.05 level (1-tailed).

** Correlation is significant at the 0.01 level (1-talied).

While the correlations provide a basic indication of the relationships between the variables, a strictly confirmatory path analysis was completed on the structural model. Figure 1 shows the path diagram of the maximum likelihood analysis. The path coefficients shown in Figure 1 represent standardized regression weights between the variables ( ). Estimates of squared multiple correlations (R2) are shown for the endogenous variables. As seen in Figure 1, the structural model

accounted for 29% of the variance in effectiveness and 59% of the variance in self-efficacy. The Chi-square statistic is significant and the Goodness of Fit index was unacceptable at .758.

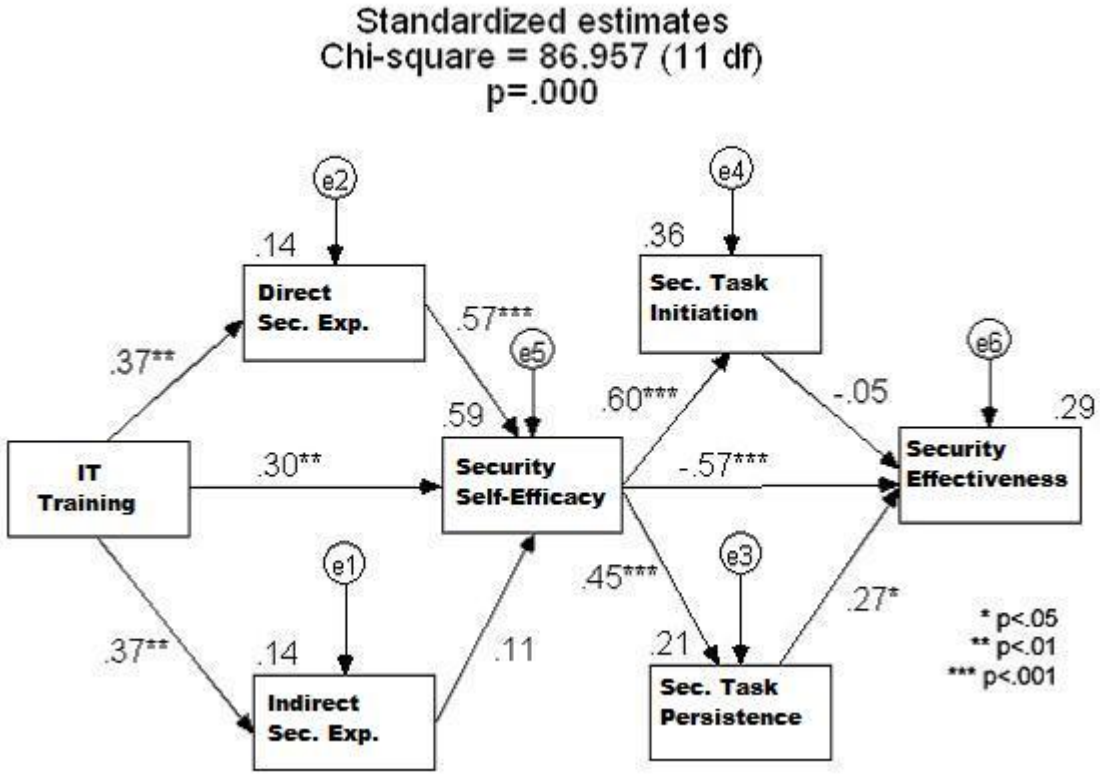

Figure 1: Path Analysis of Information System Security Effectiveness Model

Hypothesis 2a examined the relationship between information technology training and information system security self-efficacy as moderated by experience, both direct and indirect. The first relationships examined were the path coefficients between information technology training and experience, both direct and indirect. The coefficients between information technology training and both direct and indirect experience were significant (β=.37, p<.01). The coefficient between direct experience and self-efficacy was also significant (β=.57, p<.001), but the coefficient between indirect experience and self-efficacy was not (β=.11, p>.05). A path was also drawn directly between information technology training and self-efficacy. As expected, the direct relationship was significant (β=.30, p<.01), but not as strong as between information technology training and the moderators of direct and indirect information system security experience. Therefore, hypothesis 2a was partially supported. Together, information technology training, direct experience, and indirect experience accounted for 59% of the observed variance in self-efficacy.

Hypotheses 2b examined the relationship between information system security self-efficacy and information system security effectiveness, moderated by task initiation and task persistence. Again, the first relationships examined were the path coefficients between self-efficacy and task initiation and persistence. The path coefficients indicate a significant relationship for both task initiation (β=.60, p<.001) and task persistence (β=.45, p<.001). The path coefficient between task initiation (β=-.05, p>.05) and effectiveness was not found to be significant, while the coefficient between task persistence (β=.27, p<.05) and effectiveness was weak, yet significant. The path between information system security self-efficacy and information system security implementation effectiveness, however, was very strong and quite significant (β=-.57, p<.001). Therefore, although there were significant relationships between self-efficacy and both task initiation and persistence, the lack of a significant relationship between task initiation and effectiveness left the hypothesis only partially supported. Together, self-efficacy, task initiation, and task persistence accounted for 29% of the variance in effectiveness.

DISCUSSION

The primary objectives of this study were to determine if Florida systems librarians with information technology training were more effective at implementing information system security than those without and to examine the relationship between information technology training and information system security effectiveness for Florida systems librarians based on a model derived from Social Cognitive Theory. The findings of the study suggest that prior IT training is positively related to information security implementation effectiveness and that information system security self-efficacy is positively related to information system security implementation effectiveness. Other variables, such as age, gender, and job experience were also examined but are not reported here.

Information Technology Training

IT education and training vary in both breadth and depth, and as such, it is difficult to specify exactly what constituent parts are the defining factors in the demonstrated improvement in information system security effectiveness. Though this study utilized questions that could differentiate between receipt of a degree in an information technology area and 'other' information technology training, for analysis, they were considered together. Additionally, variation in the quality of training, including, as indicated in research by Gist (1989), whether the training was model based or tutorial based, may also play a role in the ultimate success of the participant and was not considered in this study.

Because the exact type of training was not specified, it is important to consider that the measurement of information system security effectiveness may have been due to awareness, not necessarily skills derived from the formal IT training, which is why awareness training is an important component of security programs and is differentiated from both skills training and education. The U.S. National Institute for Standards and Technology divides recommended security programs into three areas; awareness training, skills training, and education. Security awareness is the foundation of any security program and is intended to provide the individual with enough information to recognize potential security problems. Specifically, "Awareness stimulates and motivates those being trained to care about security and to remind them of important security practices. Explaining what happens to an organization, its mission, customers, and employees if security fails motivates people to take security seriously" (National Institute of Technology, 1995). Security training, the second level in the security program, imparts specific skills required by the audience to effectively perform their jobs in a secure manner. The highest level in the security program is security education, "[Which] is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security" (National Institute of Technology, 1995). At the lowest level of the security program, awareness is stressed so that individuals do not make poor information security choices, as seen in the work by Stanton, et. al. (2005). Although this research asked the participants about their previous formal IT training, it is possible that it was not skills training that had an affect, but awareness of the threats to and inherent vulnerabilities of the systems that caused the changes in the behavior and information system security implementation.

Direct and Indirect Information System Security Experience

An examination of the results of the study failed to offer complete support for the model. This is particularly true for the theorized mediators between information system security self-efficacy and information system security implementation effectiveness. Direct and indirect experience were highly correlated with each other, which is reasonable considering that in most instances, any direct experience is probably predicated by indirect experience. In the analysis, direct experience demonstrated a stronger relationship to self-efficacy than did indirect experience, with indirect experience alone being marginal in its predictive power.

Information System Security Task Initiation

The second set of constructs in the model were task initiation and task persistence. The measurement of task initiation was derived from previous studies and measured the number of hours per week the subject spent engaged in information system security work. While self-efficacy had significant predictive value for this construct, task initiation did not demonstrate significant predictive value for effectiveness. There are many possible reasons for this. The literature already reflects the diversification of systems librarian responsibilities as it does for those responsible for small businesses, so even if the respondent wanted to spend more time engaged in information system security activity, the finite limit on time in conjunction with other responsibilities may well temper this measurement. The effectiveness of the information system security implementation may also play a role. If the security implementation is effective, there may not be a need to spend as much time engaged specifically in the activity as there may be for a respondent with a less effective implementation. As discussed in research done by Straub (1986, 1990), implementation of appropriate preventive measures may be more effective at reducing such violations, and therefore, freeing the respondent from spending as much time each week dealing with security.

Information System Security Task Persistence

Task persistence was measured through a question that asked the respondent to state what they would do in a hypothetical situation in which they experienced difficulty establishing, configuring, or maintaining information system security. Although there was discrimination among the responses, and the correlation with self-efficacy was significant, it did not emerge as a significant predictor of effectiveness. It could be that this was not a valid measurement of persistence, even though it had face validity. It appears that some respondents inflated their sense of persistence, as it was expected that few, if any, respondents would have chosen the first possible response that stated that the respondent would, "persist with the task, until you have accounted for all the known system vulnerabilities and attempt to discover new, potential vulnerabilities in the system." In fact, nine respondents indicated that as a response. While this is possible, it is not highly plausible. Additionally, twelve respondents indicated that they would persist until they have accounted for all known vulnerabilities in the system. Since many known system vulnerabilities may not be significant to a particular implementation of the system, and other vulnerabilities may require such extreme methods to exploit that the effort required to control that vulnerability is not worth the effort, either financial or in terms of time, it appears that for this choice respondents either misinterpreted the choice or artificially inflated their true level of persistence as well.

Information Security Self-Efficacy

Taken as a whole, the model provides support for the role of self-efficacy on performance. Those respondents that had formal information technology training had significantly higher levels of, and significant predictive value for, information system security self-efficacy. Information system self-efficacy, in turn, was a valuable predictor for information system security effectiveness. As discussed earlier, the predicted mediators for self-efficacy: direct and indirect experience, task initiation, and task persistence, did not all relate as expected. While this study was conducted with systems librarians, the practical considerations of this research lie not only in the population studied, but also to the importance of information system security training and self-efficacy in any population. As discussed in the introduction, there are many similarities between small business IT management and that found in libraries. Although it is recognized that the response rate did not reach the level where the results of the study can be generalized beyond the respondents, it remains an important indicator for further study.

Any organization that employs individuals to maintain their system security can benefit from ensuring that those individuals feel efficacious in their domain of work. Hiring individuals that have had formal training in this area, or ensuring that those employed receive direct mastery experience, will help to ensure that the employees will actively engage and persist in activities related to their responsibilities, and as such, will provide a more effective implementation of security. Future research in this area should consider modifying the measurement instrument to ensure construct validity. This is particularly true for measuring task initiation and persistence. Additionally, repeating this research with other populations and with a larger sample size will enable generalization beyond what was possible with this research effort. Examination of other predictors beyond information technology training, such as organizational factors that influence information system security self-efficacy and effectiveness, would be appropriate.

Within the population studied, further research into the training of systems librarians, identifying the specific domains of information technology training that are most applicable to systems librarians, including their training in information system security, would advance the understanding of how current educational programs could be modified to improve the effectiveness of future systems librarians.

CONCLUSION

This research has attempted to demonstrate the impact of information technology training on the effectiveness of information system security implementations. It has utilized the construct of self-efficacy from Social Cognitive Theory to provide a causal link to the correlations involved. The results indicate that self-efficacy adds to our understanding of the relationship between training and effectiveness, particularly in the domain of information system security. In addition, the research has provided a tested model for further exploration of this relationship.

REFERENCES

1. Armstrong, J. S. & Overton, T. (1977). Estimating Nonresponse Bias in Mail Surveys. Journal of Marketing, 51, 71-86.
2. Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavioral Change. Psychological Review, 84, 191-215.
3. Bandura, A. (1986). Social Foundations of Thought and Action: A Social Cognitive Theory. Prentice-Hall.

4. Bandura, A. (1994). Self-Efficacy. In V.S.Ramachaudran (Ed.), Encyclopedia of Human Behavior (pp. 71-81). New York: Academic Press.
5. Barling, J. & Beatie, R. (1983). Self-Efficacy Beliefs and Sales Performance. Journal of Organizational Behavior Mangement, 5, 51.
6. Betz, N. E. & Hackett, G. (1981). The Relationship of Career-Related Self-Efficacy Expectations to Perceived Career Options in College Women and Men. Journal of Counseling Psychology, 38, 417-452.
7. Biever, E. J. (1997). Securing Public Workstations by Maintaining Software Centrally. Library Hi Tech, 15:1-2, 27-29.
8. Brakel, G. (1997). Public Workstation Security. Library Hi Tech, 15:1-2, 24-26.
9. Brandt, D. S. (2003). A Different Spin on Security. Computers in Libraries, 23, 34-36.
10. Breeding, M. (1997). Designing Secure Library Networks. Library Hi Tech, 15:1-2, 11-20.
11. Brown, I. & Inouye, D. K. (1978). Learned Helplessness Through Modeling: The Role of Perceived Similarity in Competence. Journal of Personality and Social Psychology, 36, 900-908.
12. Collins, J. L. (1982). Self Efficacy and Ability in Achievement Behavior. In New York: American Educational Research Association.
13. CompTIA (2006). Forth Annual CompTIA Study on Information Security and the Workforce. CompTIA website http://www.comptia.org/about/pressroom/get pr.aspx?prid=903. Accessed 11 April 2006.
14. Creswell, J. W. (1994). Research Design : Qualitative and Quantitative Approaches. Sage Publications.
15. Fore, J. A. (1997). Things That Go "Bump" in the Virtual Night. Library Hi Tech, 15:1-2, 84-91.
16. Garrison, W. V. & McClellan, G. A. (1997). Tao of Gateway: Providing Internet Access to Licensed Databases. Library Hi Tech, 15:1-2, 39-54.
17. German, G. (1997). To Catch a Hacker. Library Hi Tech, 15:1-2, 96-98.
18. Gist, M., Schwoerer, C., & Rosen, B. (1989). Effects of Alternative Training Methods on Self-Efficacy and Performance in Computer Software Training. Journal of Applied Psychology, 74, 884-891.
19. Gupta, A. & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. Information Management & Computer Security, 13, 297.
20. Kabay, M. E. (2005). Improving Information Assurance Education Key to Improving Secure(ity) Management. Journal of Network and Systems Management, 13, 247.
21. Koga, J. S. (1990). Security and the PC-Based Public Workstation. Online, 14, 63-70.
22. Locke, E. A., Frederick, E., Lee, C., & Bobko, P. (1984). Effect of Self-Efficacy, Goals, and Task Strategies on Task Performance. Journal of Applied Psychology, 69, 241-251.
23. Lynch, C. (1997). The Changing Role in a Networked Information Environment. Library Hi Tech, 15:1-2, 30-38.
24. Marmion, D. (1997). A Commercial Software Approach to Workstation Security. Library Hi Tech, 15:1-2, 21-23.
25. Muir, S. (1997). After the Break in Occurs: How to Handle the Student Hacker. Library Hi Tech, 15:1-2, 92-95.
26. Multon, K. D., Brown, S. D., & Lent, R. W. (1991). Relation of Self-Efficacy Beliefs to Academic Outcomes - A Meta-Analytic Investigation. Journal of Counseling Psychology, 38, 30-38.
27. National Institute of Technology (1995). Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook.
28. Newby, G. (2000). Information Security for Libraries.
29. Robertson, G. (2003). Investigating Risk: Assessing and Analyzing Trouble Before It Strikes. Library Mosaics, 14, 18-19.
30. Rosaschi, J. (1997). Give Yourself a Break; Don't give the Hackers One. Library Hi Tech, 15:1-2, 99-102.
31. Schultz, E. (2004). Security training and awareness—fitting a square peg in a round hole. Computers & Security, 23,

1-2.

32. Schunk, D. H. (1981). Modeling and Attributional Effects on Children's Acheivement: A Self-Efficacy Analysis. Journal of Educational Psychology, 73, 93-105.
33. SPSS, i. (1999). SPSS Base 9.0: Applications Guide. Chicago: SPSS.
34. Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24, 124.
35. Straub, D. (1986). Controlling Computer Abuse: An Empirical Study of Effective Security Countermeasures. DBA Indiana University.
36. Straub, D. (1990). Effective IS Security: An Empirical Study. Information Systems Research, 1, 255-276.
37. Stumpf, S. A., Brief, A. P., & Hartman, K. (1987). Self-Efficacy Expectations and Coping with Career-Related Events. Journal of Vocational Behavior, 31, 91-108.
38. Wade, J. (2004). The Weak Link in IT Security. Risk Management, 51, 32-37.
39. Wang, A. Y. & Newlin, M. H. (2002). Predictors of web-student performance: the role of self-efficacy and reasons for taking an on-line class. Computers in Human Behavior, 18, 151-163.
40. Wood, R. & Bandura, A. (1989). Social Cognitive Theory of Organizational Management. Academy of Management Review, 14, 361-384.
41. Xu, H. & Chen, H. (1999). What do Employers Expect? The Educating Systems Librarian Research Project 1. The Electronic Library, 17, 171-179.
42. Xu, H. & Chen, H. (2000). Can We Meet The Challenge? The Educating Systems Librarian Research Project 3. The Electronic Library, 19, 315-327.
43. Xu, H. & Chen, H. (2000). Whom Do Employers Actually Hire? The Educating Systems Librarian Research Project Report 2. The Electronic Library, 18, 171-182.
44. Young, M., Kyrillidou, M., & Blixrud, J. (2002). ARL Supplementary Statistics Washington, D.C.: Association of Research Libraries.