Social Engineering Self-Efficacy: Social Engineering Awareness, Recognition, and Response

ABSTRACT

Very little research information systems research has focused on social engineering attacks. Social engineers use tactics that make many technical and bureaucratic controls inefficacious. This paper proposes and tests a theoretical construct—social engineering self-efficacy (SESE)—to be used in future research.

Keywords

social engineering, social cognitive theory, self-efficacy, information security

INTRODUCTION

Information system (IS) security breaches are harmful to organizations and their clients. The Computer Security Institute (CSI) reports that, on average, organizations lose more than $200,000 annually to security issues . Similarly, CSI reports that IS security spending is increasing, from 12.8% of an organization's IT budget in 2009 to 18.6% in 2010 . IS security researchers have examined many methods to reduce security breaches, such as the development of technical controls, and internal IS security policies and security awareness and ethics training programs. Little attention, however, has been paid to social engineering attacks, and even less attention to the development of theory surrounding social engineering . This is troublesome given that organizational insiders are the weak link in securing information systems and social engineers focus almost exclusively on manipulating the human element. This paper, therefore, proposes a construct to examine social engineering—social engineering self-efficacy.

Social engineering describes strategies used to exploit social structures and biases to manipulate people into engaging in specified behaviors such as divulging confidential information . Social engineers use many tactics to manipulate their victims. Phishing, for example, is a social engineering strategy in which the social engineer seeks to attain confidential information from victims by masquerading as a legitimate and trustworthy entity. In 2007, phishing attacks affected more than 2 million victims, creating more than $3 billion in losses . Similarly, social engineers may offer prizes for the disclosure of information . Some individuals may even knowingly trade confidential information for relatively small rewards . Clearly, social engineering attacks have the potential to easily defraud individuals.

This paper argues that the development of self-efficacy related to social engineering will diminish human security vulnerabilities. Self-efficacy is a concept derived from Bandura's social cognitive theory . Self-efficacy refers to individuals' "judgments of their capabilities to organize and execute courses of action required to attain designated types of performances" . The foundation of social cognitive theory, and therefore self-efficacy, is based on a reciprocal interaction between three factors: (1) personal factors in the form of cognitions and affects which include motivational factors such as self-efficacy and anxiety; (2) behavioral factors in the form of strategies which include the cognitive strategies of integrating and metacognitive strategies of monitoring and regulating ; and (3) environmental influences and factors such as formal and informal policies and regulations . Bandura posits that humans possess cognitive means and capabilities to make sense of their own experiences and the experiences of others through self-reflection and observation, and thus, to alter their thinking and behavior.

The remainder of this paper explores the construct of self-efficacy in a social engineering context. First, this paper presents the development of the social engineering self-efficacy construct. Second, this paper describes the methodology used to test the construct. Third, this paper examines the results of a partial least squares (PLS) analysis on data collected from hospital nurses. Finally, this paper offers implications of social engineering self-efficacy and directions for future research.

CONCEPTUAL MODEL

IS security studies have primarily ignored social engineering research, particularly with regard to theory development . This paper attempts to further bridge this gap by introducing a new construct—social engineering self-efficacy (SESE)—to be used in future research. This paper conceptualizes SESE as consisting of three types of efficacy—awareness self-efficacy, recognition self-efficacy, and response self-efficacy. Together, these three types of efficacy and the relationships between them constitute social engineering self-efficacy. Social engineering self-efficacy (SESE), therefore, refers to individuals'

confidence in their abilities to generate awareness of social engineering tactics, recognize social engineering attacks, and develop appropriate responses to those attacks by acquiring and utilizing cognitive, social, and material resources.

Awareness Self-efficacy

Fostering employee awareness of information security is an important step in securing information systems in organizations. Bulgurcu, Cavusoglu, and Benbasat , for example, found that awareness of information security policies (ISP) and general awareness of security practices improves attitudes toward complying with an ISP, and therefore, garners compliance with the ISP. Similarly, Dinev and Hu showed that awareness of protective technologies influences attitudes toward the technologies, thereby increasing intentions to use them. In a similar fashion, this paper argues that an individual's perceptions that he/she can become aware of social engineering tactics and countermeasures will increase the individual's perceptions of efficacy to act in a proactive manner when faced with social engineering in the workplace.

In this paper, awareness self-efficacy refers to an individual's perceptions that he/she can acquire and utilize cognitive and other resources to improve his/her knowledge and understanding of social engineering tactics and countermeasures. Social cognitive theory suggests that individuals with high self-efficacy will exert more effort toward completing a task, while individuals with low self-efficacy may exert less effort or avoid the task completely . Thus, when awareness self-efficacy is high, individuals will be more likely to remain engaged in learning about potential attacks and countermeasures during awareness training, and be more likely to independently search for information about social engineering. Importantly, self-efficacy has been shown to affect learning .

Those with low awareness self-efficacy, however, may be less likely to remain engaged during awareness training and more likely to avoid potential opportunities to learn more about social engineering. Individuals with low self-efficacy may believe tasks are more difficult than they truly are. Such beliefs foster anxiety and a narrow vision of how best to engage a task . Thus, there is a reciprocal relationship between self-efficacy and anxiety. People who do not have high efficacy beliefs may readily experience feelings of anxiety. Conversely, anxiety about a subject such as information security or social engineering attacks may induce low efficacy perceptions in people. If awareness training, therefore, prompts feelings of anxiety, individuals' perceptions of their ability to learn about social engineering may be diminished.

Recognition Self-efficacy

Being able to recognize social engineering attacks increases the likelihood that responses to attacks will be proactive. Social engineering attacks may be difficult to recognize. Social engineers use existing social structures to deceive victims; therefore, unsuspecting victims may not even realize that an attack is occurring. This paper assumes that recognition is a skill that can be acquired and that individuals develop efficacy perceptions related to recognition. Workman , for example, suggests that "training can assist people [to know] what to look for before trusting [people]" , especially in an online setting. Recognition self-efficacy, therefore, refers to an individual's perceptions that he/she would be able to recognize a social engineering attack if an attack occurred in the workplace.

This paper submits that awareness self-efficacy has an effect on recognition self-efficacy. A person with high awareness self-efficacy is likely to understand more about social engineering tactics than a person with low awareness self-efficacy. The level of knowledge and understanding a person has regarding social engineering tactics will improve the individual's ability to recognize those tactics when employed by a social engineer. This does not suggest, however, that a person must have awareness about social engineering tactics to recognize them. General understanding of persuasion and influence or intuition may also improve recognition. Thus, this paper offers the following hypothesis:

H1: awareness self-efficacy has a positive relationship with recognition self-efficacy.

Response Self-efficacy

This paper submits that responses to social engineering attacks will be more effective with higher self-efficacy. Self-efficacy is key to sustaining effort in performing a given task, especially in the face of adverse conditions . This paper defines response self-efficacy as an individual's perceptions that he/she can acquire and utilize cognitive and other resources to develop responses to social engineering attacks that will enable him/her to withstand the attacks. Self-efficacy develops to the extent that individuals' reflections about task performance are positive and reaffirming . High self-efficacy helps create feelings of confidence in approaching difficult tasks and activities. In information security, self-efficacy has been shown to affect intentions to comply with information security policies . This paper argues in similar fashion that high levels of response self-efficacy will increase proactive reliance on appropriate countermeasures to social engineering attacks.

Awareness self-efficacy may affect response self-efficacy. Without awareness of social engineering countermeasures, it would be difficult for an individual to develop effective coping strategies for handling social engineering attacks. As awareness self-efficacy increases, awareness of social engineering countermeasures is likely to increase as well. Importantly, task knowledge is important in developing confidence in task completion . Therefore, awareness self-efficacy will improve response self-efficacy by increasing knowledge of coping mechanisms. Thus, this paper offers the following hypothesis:

H2: awareness self-efficacy has a positive relationship with response self-efficacy.

Recognition self-efficacy may also affect response self-efficacy. Without recognition self-efficacy, an individual might have a hard time recognizing an attack. Self-efficacy is increased by positive experiences with a task and is decreased with negative experiences . Therefore, an individual's response self-efficacy might decrease after learning that an attack occurred and the individual failed to recognize it and act appropriately. The opposite is likely to be true for individuals with high recognition self-efficacy. The ability to recognize an attack is the first step to preventing it. This paper therefore submits the following hypothesis:

H3: recognition self-efficacy has a positive relationship with response self-efficacy.

Social Engineering Self-Efficacy

Social engineering self-efficacy (SESE) consists of efficacy perceptions related to garnering awareness of social engineering tactics and countermeasures, developing recognition skills, and developing coping mechanisms to counter social engineering attacks. Table 1 presents the definitions of these constructs. Importantly, these three types of efficacy interact as described above to form SESE. Importantly, SESE is only part of a larger nomological net. Figure 1 depicts the interactions between awareness, recognition, and response self-efficacy in the nomological net of social cognitive theory.

Table 1 - Definitions of Key Constructs

Construct	Definition
Social engineering self-efficacy	Individuals' confidence in their abilities to generate awareness of social engineering tactics, recognize social engineering attacks, and develop appropriate responses to those attacks by acquiring and utilizing cognitive, social, and material resources.
Awareness self-efficacy	Individuals' perceptions that they can acquire and utilize cognitive and other resources to improve their knowledge and understanding of social engineering tactics and countermeasures.
Recognition self-efficacy	Individuals' perceptions that they would be able to recognize social engineering attacks.
Response self-efficacy	Individuals' perceptions that they can acquire and utilize cognitive and other resources to develop responses to social engineering attacks that will enable them to withstand the attacks.

For example, as depicted in Figure 1, SESE is likely to be affected by constructs specified by social cognitive theory. The development of self-efficacy toward a task has been shown to be a function of prior experience with the task, vicarious experience through observation, persuasion, and emotional arousal. Prior experience is the most influential factor in developing self-efficacy . Social engineering self-efficacy, therefore, is likely to increase with successful: learning experiences, recognition of engineering attacks, and responses to attacks. Conversely, self-efficacy is likely to decrease with failed attempts to understand social engineering, recognize attacks, and generate response to attacks. Besides experience with social engineering attacks, training may also be useful. Training which includes multiple sources of efficacy, such as elements of persuasion and modeling appropriate behavior (vicarious experience), may be more effective than training that just focuses on persuasion.

Ultimately, this paper suggests that high SESE will increase the likelihood that individuals will react proactively and appropriately to social engineering attacks. Self-efficacy has been a strong predictor of appropriate behavior, and therefore, successful outcomes in many and varied studies . Organizations, therefore, should seek to engender SESE beliefs in their

employees. To the extent that organizations are successful in this endeavor and other security controls are in place, information security will increase.

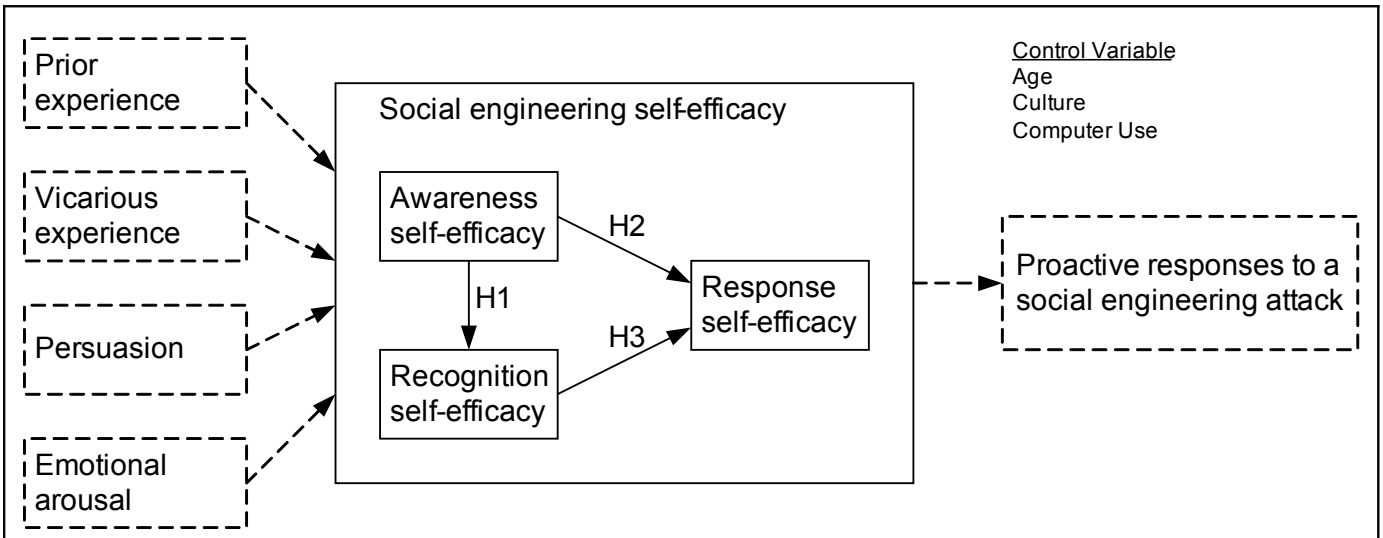

Figure 1. Social Engineering Self-Efficacy in Social Cognitive Theory Nomological Net

METHODOLOGY

To test the relationships between awareness, recognition, and response self-efficacy, a paper survey was developed and distributed to 206 nurses in a hospital in the southeastern United States. The survey was administered during a yearly training and certification program and the researchers had a booth at the training session; therefore, the survey received an extremely high response rate and garnered responses from a variety of nursing fields (e.g., orthopedics, pediatrics, intensive care, etc.). Nurses were used as they have regular access to confidential information made available through information systems.

Measures for awareness, recognition, and response self-efficacy were adapted from other studies. Table 2 presents the items for each of the three self-efficacy constructs. Control variables were included for age, gender, computer and network use, culture, and work setting. All items were measured on a 5 point Likert scale from strongly disagree to strongly agree. Data analysis was conducted using partial least squares (PLS) with SmartPLS (Version 2.0).

Table 2 - Measurement Items For Self-efficacy Constructs

Item	Question
REC-SE1	I am confident that I can identify unauthorized access to medical records.
REC-SE2	I am confident that I can identify unauthorized use of medical records.
REC-SE3	I am confident that I can identify unauthorized disclosure of medical records.
REC-SE4	I am confident that I can identify unauthorized access to institution network.
REC-SE5	I am confident that I can identify unauthorized use of institution network.
REC-SE6	I am confident that I can identify unauthorized modification to institution network.
RESP-SE1	I am confident that I can take appropriate actions upon discovering unauthorized computer or network activity.
RESP-SE2	I am confident that I can allow only appropriate physical access to computers.
RESP-SE3	I am confident that I have the necessary skills to protect myself from information security

	violations.
RESP-SE4	I am confident that I have the skills to implement the available preventative measures to stop people from getting my confidential information.
RESP-SE5	I am confident that I have the skills to implement the available preventative measures to stop people from damaging my system.
AWR-SE1	I am aware of what to do in the event of an information security breach even if there is no one to tell me what to do.
AWR-SE2	I am aware of what to do in the event of an information security breach, even if I do not have a copy of written procedures and rules to refer to.

Participants

Survey participants were primarily female nurses (94 percent female). The average age of the nurses was 43, ranging from 19 to 70. 9 percent of the nurses had a acquired a high school diploma, 30 percent had acquired an Associate's Degree, 46 percent had acquired a Bachelor's Degree, 14 percent had acquired a Master's Degree, and 2 percent had acquired a PhD. 98 percent of the nurses admitted to using computers and networks in their work. On average, nurses reported that they spend at least 20 to 50 percent of their day using computer systems. The majority of nurses used the computer systems primarily to access patient information and help with the practice of nursing. The computer usage statistics suggest that nurses' regular access to patient information presents the potential for social engineering attacks targeted at nurses to gain access to protected healthcare information.

RESULTS

Since the model in this paper is extremely parsimonious and paths lead almost exclusively to a single variable, multiple regression analysis was used to determine a good fitting model before exploring further relationships with PLS. Adjusted R^2 values, Cp, BIC, and AIC values from the multiple regression suggest that the most fitting model for response self-efficacy includes awareness self-efficacy, recognition self-efficacy, age, culture, and the portion of time nurses spend on computer systems. All other control variables demonstrated no evidence of an effect on response self-efficacy.

Overall, the model shows high reliability. Composite reliabilities for the model ranged from 0.87 to 0.96, suggesting acceptable levels of internal consistency. Additionally, average variance extracted (AVE) for all latent variables was higher than 0.50, ranging from 0.58 to 0.90. These values are depicted in Table 3.

Table 3 - Composite Reliability and AVE

	Composite reliability	**Average variance extracted**
Awareness	0.95	0.90
Recognition	0.96	0.80
Response	0.87	0.58

Discriminant validity was tested by comparing the squared correlations between latent constructs with corresponding values of AVE. Table 4 shows the latent variable correlations with AVE down the diagonals. In all cases, the squared correlations were lower than the AVE for the corresponding latent variables. This suggests the measurement model has discriminant validity.

Table 4 - Latent Variable Correlations with AVE on Diagonals

	Awareness	**Recognition**	**Response**
Awareness	0.90		

Recognition	0.34	0.80	
Response	0.63	0.44	0.58

Item cross-loadings were calculated in SmartPLS. The results are shown in Table 5. All items loaded higher on their principal construct than on any other construct. All but two factors had loadings greater than 0.80. Two of the five items for response self-efficacy loaded lower at 0.55 and 0.68. Further, t-values for each factor loading on its principal construct show significant loadings as depicted in Table 5.

Table 5 - Factor Loadings (bolded) and Cross-loadings

	Awareness	**Recognition**	**Response**	**T-value**
REC-SE1	0.27	**0.88**	0.34	23.08
REC-SE2	0.23	**0.89**	0.31	23.28
REC-SE3	0.20	**0.83**	0.27	16.52
REC-SE4	0.34	**0.93**	0.44	49.07
REC-SE5	0.33	**0.93**	0.44	41.81
REC-SE6	0.38	**0.89**	0.47	33.13
RESP-SE1	0.44	0.41	**0.55**	5.68
RESP-SE2	0.40	0.26	**0.68**	8.61
RESP-SE3	0.51	0.38	**0.84**	24.41
RESP-SE4	0.50	0.31	**0.85**	22.49
RESP-SE5	0.56	0.31	**0.85**	23.01
AWR-SE1	**0.96**	0.34	0.66	105.29
AWR-SE2	**0.94**	0.31	0.52	40.87

Structural Model

PLS was conducted in SmartPLS to test the hypotheses described above. Figure 2 depicts the results. Convincing evidence exists to suggest that awareness self-efficacy affects recognition self-efficacy (beta = 0.34; t-value = 3.79). This offers support for H1. Further, convincing evidence exists to suggest that awareness self-efficacy affects response self-efficacy (beta = 0.54; t-value = 7.54). This offers support for H2. Convincing evidence also exists to suggest that recognition self-efficacy affects response self-efficacy (beta = 0.24; t-value = 2.56). Support, therefore, exists for H3 as well. Age also exhibited strong evidence of an effect on response self-efficacy (beta = -0.16; t-value = 2.17), while computer use showed suggestive yet inconclusive evidence of an effect (beta = 0.13; t-value 1.73). The negative path coefficient for age may be due to anxiety older generations experience related to computer security. Convincing evidence does not exist to suggest that culture effected response self-efficacy (beta = 0.08; t-value = 0.94).

Together, awareness self-efficacy and recognition self-efficacy account for a relatively large portion of the variance in response self-efficacy. A multiple regression analysis with the control variables results in an R^2 of 0.51 and an adjusted R^2 of 0.49. Whereas, without the control variables, awareness self-efficacy and recognition self-efficacy still result in an R^2 of 0.45 and an adjusted R^2 of 0.44. The PLS model shows similar results, from an R^2 of 0.51 with control variables to an R^2 of 0.46 without. Awareness and recognition self-efficacy, therefore, seem to be strong predictors of response self-efficacy. The effect of awareness self-efficacy on recognition self-efficacy yielded an R^2 of 0.12.

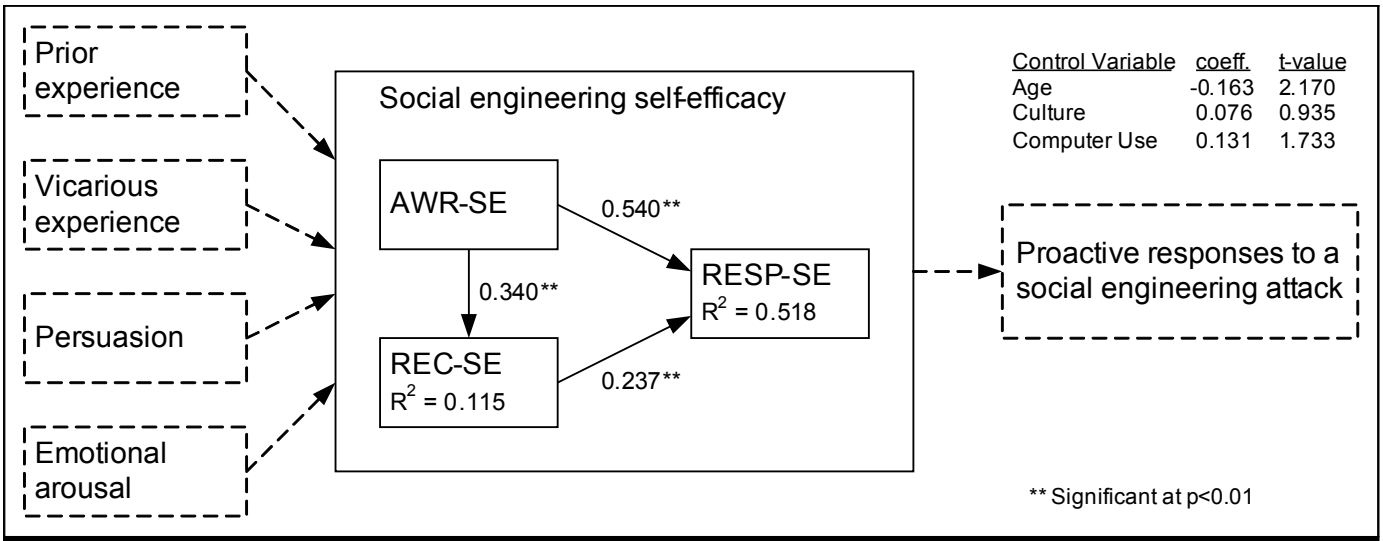

Figure 2. Results of PLS Analysis

DISCUSSION AND IMPLICATIONS

This paper has argued for the use of a new construct in social engineering research. Due to the lack of theory in social engineering research, this construct should prove useful in examining and developing successful training programs, examining resilience to social engineering attacks, and explaining the development of successful responses to attacks. This paper has suggested that SESE consists of three types of efficacy which interact to create the whole. These types of efficacy include awareness self-efficacy, recognition self-efficacy, and response self-efficacy. In order to develop appropriate responses to social engineering attacks, individuals may need to develop high awareness self-efficacy and recognition self-efficacy.

Initial results from an analysis conducted on nurses in a hospital setting suggest that awareness self-efficacy and recognition self-efficacy do alter perceptions of an individual's ability to develop and deploy appropriate responses. This suggests that the development of effective training programs that employ persuasion and modeling techniques may help to increase employees' abilities to cope with social engineering attacks. In the healthcare setting, developing SESE may be particularly important, as the analysis above suggests that nurses frequently access protected healthcare information.

Limitations and Future Research

The primary purpose of this paper was to introduce a new construct for studying social engineering. Although this paper has shown how the three types of efficacy—awareness, recognition, and response—interact, this paper has not tested the effect of SESE on actual performance. Similarly, this paper has addressed possible sources for developing SESE, but has not tested these. However, these limitations present ample room for future research. Future studies could examine the effect of SESE on actual performance through an experimental design. Similarly, theories of training for social engineering could be developed and tested using the SESE construct.

Although the sample in this study garnered nurses from multiple fields, most of the nurses were hospital nurses. Similarly, the nurses were all from the same geographic area. Nursing was also the only profession used in the study. This suggests that the results may not be extremely generalizable. Future research should examine more industries from a more diverse, randomly sampled population. Although this paper has focused on organizational attacks, SESE is likely to be an effective predictor of proactive and appropriate behaviors for home computer users as well. Future research might also consider using SESE to examine personal computing habits.

Lastly, this study used a non-experimental design. Although the findings suggest evidence of a relationship between the types of efficacy, they do not suggest causality. Future research might examine these variables in an experimental setting to further test the causal links between these variables. Future research might pay particular attention to the relationship awareness self-efficacy and recognition self-efficacy to determine if it is indeed a reciprocal relationship.

Conclusion

More research needs to be conducted on social engineering as humans are the weak element in information security. It is likely that social engineers will continue to develop and improve tactics for gaining behavioral compliance and information disclosure. Researchers and practitioners alike, therefore, must continually seek new methods to fight against social engineers. This paper offers a construct that can be used to further develop countermeasures and effect programs to train employees.

REFERENCES

Acquisti, A., & Grossklags, J. (2003). *Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior.* Paper presented at the 2nd Annual Workshop on Economics and Information Security (WEIS'03), Berkeley, CA.

Bandura, A. (1977a). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215.

Bandura, A. (1977b). *Social learning theory*. Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. (1997). *Self-efficacy: The Exercise of Control*. New York, NY: Freeman.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Clark, R. C., & Mayer, R. E. (2003). *E-learning and the Science of Instruction*. San Francisco, CA: Jossey-Bass.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386-408.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*, 106-125.

McCall, T. (2007). Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks Retrieved Feb 24, 2012, 2012

Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York, NY: Wiley.

Pajares, F., & Miller, M. D. (1994). Role of self-efficacy and self-concept beliefs in mathematical problem solving: a path analysis. *Journal of Education Psychology, 86*(2), 193-203.

Richardson, R. (2009). 14th annual CSI computer crime and security survey (pp. 1-14): Computer Security Institute.

Richardson, R. (2011). 15th Annual 2010/2011 Computer Crime and Security Survey (pp. 1-44): Computer Security Institute.

Schommer, M., Crouse, A., & Rhodes, N. (1992). Epistemological beliefs and mathematical text comprehension: Believing it is simple does not make it so. *Journal of Education Psychology, 82*, 435-443.

Schunk, D. H., & Pajares, F. (2005). Competence Perceptions and Academic Functioning In A. J. Elliot & C. C. Dweck (Eds.), *Handbook of Competence and Motivation* (pp. 85-104). New York, NY: Guilford Press.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*, 101-105.

Wlodkowski, R. J. (1999). *Enhancing Adult Motivation to Learn*. San Francisco, CA: Jossey-Bass.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: a study of insider security contravention. *Journal of the American Society for Information Science and Technology, 58*(2), 212-222.