Protection Motivation Driven Security Learning

Research-in-Progress

Yi Ding
Georgia Gwinnett College
yding1@ggc.edu

Peter Meso
Georgia Gwinnett College
pmeso@ggc.edu

Shuting Xu
Georgia Gwinnett College
sxu@ggc.edu

Abstract (Required)

In this study, we present a research in progress report of our development of information security hands on exercises based on protection motivation theory (PMT) to promote security learning motivation and outcomes. This report also includes a preliminary evaluation that contrasts our PMT driven hands on approach with traditional lecture approach and examines their difference on influencing a subject's security learning motivation and performance during information security awareness training. Overall, our study not only demonstrates the application of PMT into security training hands on exercise development that promote one's better perception of security threats and coping responses but also provide partial empirical evidence supporting the use of PMT for training method development and assessment. This study would benefit those researchers, teachers, and practitioners who are interested in exploring theoretically sound ways of security training.

Keywords (Required)

Security awareness training, protection motivation theory, information security

Introduction

There is a broad consensus on the need for training and education of the current and future workforce to be able to effectively deal with present, emergent, and future cyber security challenges. Currently, information security education and training are provided in a variety of avenues, such as traditional lectures, hands-on exercises, real world simulations, online training, emails on security tips and updates, etc. However, there is a lack of studies that follow a theoretical approach to develop and assess their training methods. In this study, we report our research in progress of following the protection motivation theory (PMT) (Rogers 1975) to develop a hands-on based teaching approach with the goals to motivate and promote trainees' security learning interest and performance. Then, we assess our method by comparing it with the traditional education approach based on their influences on several key learning outcome variables, such as motivation to learn, learner satisfaction, skill development variables (Alavi and Leidner 2001).

Our study should benefit both security training professionals who are interested in developing effective training methods and researchers who are interested in better understanding of the applicability, limit, and the extensibility of protection motivation theory in information security research.

Literature Review

In higher education, information security awareness has been one of the major themes that make up college freshman level Information Systems (IS) education courses (e.g., Baltzan 2012, Kroenke 2012, Stair and Reynold 2012). Many of those IS courses covering security topics such as malware, identity theft, password-based authentication, firewall, wireless security, etc. often follow traditional lecturing approaches, which typically rely on selected textbook materials, lecture slides, papers, group discussions, etc.. Students' learning outcomes are comprehended based on their performance on "paper-based and theoretical" assignments or tests (Vigna 2003, p. 8). However, the effectiveness of such an approach has been questioned. Researchers have argued traditional lecturing often leaves "students with little understanding of application of concepts" in a real-world scenario (Riskowski et al. 2009, p. 182).

In industry, similar question exists for the effectiveness of various information security awareness training programs. To many organizations information security awareness training is considered as one of major countermeasures to achieve information assurance (e.g., Schou et al. 2004, NIST 2002). Yet, users who get trained often choose to ignore what are recommended during their practices in a real world setting (Cone et al. 2007).

In the fields of science and technology, hands-on based training has been promoted as a key tool for achieving effective learning of scientific and technological subjects (MA and Nickerson 2006). As many information security topics such as malware, password cracking, hacking, etc. are technical oriented, to improve the effectiveness of security awareness training, numerous hands-on based labs and projects have been proposed and discussed for effective security education purpose (e.g., Logan and Clarkson 2005; Hill et al. 2001; Ariyapperuma & Minhas 2005; Schembari 2007; Locasto & Sinclair 2009, etc.). While it is evident that numerous training instruments (e.g., labs, tools, simulation methods, etc.) have been developed to provide students with hands-on educational experiences (Du and Wang 2008, Shumba 2004, Stevenson and Romney 2004), most of those hands-on exercises are typically used for advanced level of security skill training (Meiselwitz 2008). To general public who have neither background nor interest in information security it has always been a challenge to find an effective security awareness training method to motivate them to not only learn basic security principles well but have a willing to apply them in a real world setting (Herath and Rao 2009, Maughan 2010).

Security game (either visual or competition based) training approaches have also been tried in different studies for security awareness education but their effectiveness have yet to be fully assessed (e.g. Cone et al. 2007, Sommers and Robinson 2004). In fact, the lack of serious effectiveness evaluation of training methods is not just an issue in security education studies but a common phenomenon among many science and engineering studies that employ hands-on approach for education purpose (MA and Nickerson 2006). Those studies tend to focus on the practical design and development of the methods or instruments. The evaluation part often tends to be brief, ad-hoc, and mostly based on self-reported qualitative feedback from students. Researchers have argued that clear, well-formed, and consistent objectives are needed for effective evaluation of hands-on learning initiatives (Lee and Carter 1972).

PMT Theory Driven Hands-on Exercise Development

According to PMT, individual has a protection intention which is motivated in response to perceived threats or dangers (Rogers 1975). According to Rogers, such motivation to respond is an outcome of a series of "cognitive mediational processes" that involve comprehension of threats and evaluation of efficacy of coping response variables. In specific, those processes "appraise the information available on perceived severity of threat, the perceived probability that threat will occur, the perceived ability of coping behavior to remove the threat (coping response efficacy), and the individual's perceived ability to carry out the coping behavior (self- efficacy)" according to PMT (Rogers 1975, pp. 37). The theory suggests that an individual is better motivated to protect when s/he believes "a recommended coping response can effectively prevent the occurrence" of a threat that s/he perceives to be dangerous and likely to happen (Rogers 1975, p. 99). One requirement for this process to work is that a subject must be able to comprehend an event appropriately whether or not as a threat. Recognizing the important role of those "cognitive mediational processes" in the fear appeal communication that "had been found to be generally effective in producing attitude change" in topics such as "cigarette smoking, dental hygiene, etc." (Maddux and Rogers 1983, p. 469 ~ 450), we develop our security training instruments with focus on promoting

appropriate perception of the security threats, their severity, and coping efficacy in order to best motivate our subjects' learning and behavior changes by as most of our subjects typically are not only lack of awareness of many information security threats and often have false confidence about their coping abilities. Our assessment of this approach would help us understand whether PMT maintains its utility in supporting information security training as it had been used and validated in other fields.

In the current research in progress we report our preliminary development and evaluation of a password security training module that follows the PMT principles. We choose the password security training as our starting point of a series of information security awareness training modules development because "passwords have become a necessary part of our everyday lives, controlling access to the systems and applications hosting digital information" (Weber et al. 2008, p. 1). Even though majority of the subjects in our training have little professional information security experience or knowledge, all of them have long password usage experience. However, such usage experience does not necessarily indicate that subjects are appropriately aware of password security threats (e.g., password cracking) and their severities. Nor does it grant subjects appropriate knowledge of how to create threat resistant password to cope with those threats. On the contrary, we expect many of our subjects not only have false perception about what makes a strong password and how strong it can be against password cracking threat but also have false confidence about how they can deal with those threats. According to PMT, subjects would not be much motivated to learn and follow recommended strong password principles and practices if they perceive the likelihood of a threat against their existing password practices is low or if they believe their existing password practices are already effective enough to deal with the threats. Therefore, to better motivate our subjects to learn in the security awareness education class, their existing beliefs and perceptions about security practices need to be challenged.

For our password hands-on exercise, subjects are first asked to create a few of passwords that they perceive as strong passwords. Then, we introduce a password cracking tool and demonstrate how to use that tool to crack an example password. Later, we ask subjects to apply what they have learned about the password cracking tool to crack those passwords they created and considered as strong passwords. It turns out many subjects are shocked to learn how easily those passwords they considered as strong can be broken in a matter of seconds or at most one or two minutes. Based their comments and feedback we believe many of them have started to question their original perceptions of what are considered as strong password practices and the how likely a password threat such as password cracking can occur and successfully break their passwords. Afterwards, we introduced strong password principles and have those subjects applied those principles to create a set of new passwords that the password cracking tool cannot easily break.

According to the PMT, we expect our subjects are much better motivated to learn password topics than they originally were after they have gone through this exercise since they now should have better comprehension of the threat and its likelihood to occur as well as the knowledge of how to cope with the threat effectively. We also expect our subjects are better motivated in general to learn other security awareness subjects as well. This is because when a subject is challenged on the part that they feel they have the most experience and confidence to deal with, s/he should be motivated to learn the recommended approaches and principles for those parts that they even have less experience and confidence to cope with effectively. Since motivation to learn is often highly correlated with the learning outcomes (Colquitt and Simmering 1998, Klein et al. 2006) we expects our subjects would demonstrate better learning outcomes better those who are taught with a non PMT driven approach such as class lecturing.

To assess the effectiveness of our model, based on the above discussion, we developed our following hypotheses to test:

Hypothesis 1: *PMT driven hands-on approach leverages the impact on motivation to learn significantly more than the conventional approaches such as class lectures do*

Hypothesis 2: *PMT driven hands-on approach leverages the impact on learning outcomes significantly more than do the conventional approaches such as class lectures do*

- Hypothesis 2a: *PMT driven hands-on approach leads to significantly more learner satisfaction than do the conventional approaches such as class lectures do*

- Hypothesis 2b: *PMT driven hands-on approach leverages the impact on skill-based learning outcomes significantly more than do the conventional approaches such as class lectures do*

Here, the motivation variable is the main dependent variable of PMT. The learning outcome variables are affective outcome variable - learner satisfaction and cognitive outcome variable - skill-based outcome variables. Those variables are often used as indicators of training effectiveness in existing studies (Kraiger 1993, Yi and Davis 2001, Klein et al. 2006).

Method

We have conducted a preliminary test to assess our hypotheses based on a posttest only, control group design. A total of 120 participants in this study were drawn from undergraduate students enrolled in a freshman level information technology course during the week of covering information security concepts. They are divided into two groups. The experimental group has 47 participants from randomly selected sections. They were given a forty minutes hands-on password exercise during the week of information security study. 73 participants in the control group were from the sections that followed the conventional class lecturing approach. Among those participants, 38% of them are in a STEM major (science, technology, engineering, and mathematics), 18% are in business major, the rest 54% of participants are from other majors such as education, liberal arts, or undeclared. All participants are regular internet users who use Internet at least more than 2 hours on a daily basis.

All participations were voluntary. At the end of the information security education week, an online survey measuring learner's motivation, satisfaction, and skill-based learning outcome was given to the class instructors in both groups to administer in their own sections of classes. The authors served as both instructors and experimenters to conduct the hands on exercise in their own sections.

Our learning outcome measures, such as skill development and learner satisfaction measures are adapted from Wan et al.'s study of self-regulated learning on e-learning outcomes (2012). Motivation to learn measures were adapted from education literature (e.g., Noe and Schmitt 1986, Colquitt et al. 1998, Klein et al. 2006). 5-point Likert scale from "strongly disagree" to "strongly agree" is used.

To test our hypotheses, simple one-tailed t-tests were performed to determine whether experimental group demonstrates significantly better results than our control group does. The mean, variance, and p values of each variable measure are reported as below.

Table 1 - Motivation to Learn Measures

	PMT Hands on Exercise (N=47)			Conventional Class Lecturing (N=73)		
	Item 1	Item 2	Item 3	Item 1	Item 2	Item 3
Mean	3.94	3.91	3.81	3.64	3.64	3.42
Variance	0.887	0.906	0.941	0.732	0.788	0.775

p values (<0.05): item 1 - 0.044*, item 2- 0.061, item 3 – 0.015*

Table 2 - Skill Development Measures

	PMT Hands on Exercise (N=47)			Conventional Class Lecturing (N=73)		
	Item 4	Item 5	Item 6	Item 4	Item 5	Item 6
Mean	4.26	4.32	4.09	4.14	3.81	3.7
Variance	0.629	0.613	0.775	0.648	0.713	0.991

p values (<0.05): item 4 - 0.215, item 5 - 0.0005**, item 6 – 0.014*

Table 3 – Learner Satisfaction Measures

	PMT Hands on Exercise (N=47)			Conventional Class Lecturing (N=73)		
	Item 7	Item 8	Item 9	Item 7	Item 8	Item 9
Mean	4.26	4.24	4.26	3.71	4.11	4.04
Variance	0.629	0.586	0.629	0.68	0.571	0.54

p values (<0.05): item 7 - 0.00024**, item 8 - 0.184, item 9 – 0.07

The t-test results show that our hypothesis 1 is largely supported. Only one motivation to learn measure fails to detect the significance of the PMT method's effect. To our surprise, our hypothesis 2a is only partially supported as two learner satisfaction measures fail to catch the impact of PMT method. However, our hypothesis 2b is largely supported as only two out of three skill development measures are able to demonstrate the significant impact of PMT effect. For those measures failed on showing significant impact of PMT method it could be due to a number of factors. One of them could be due to the small sample size that we have here.

Discussion

Although the test we conducted here is just preliminary and our analysis is also limited, the results show quite encouraging sign that our PMT driven hands-on approach can be a promising method for effective information security training. The future development of this study will include a further refine of our experiment design and tests. In specific a pretest will be formed and compared against the post test result. A number of variables such as threat appraisal variables and coping appraisal variables that we didn't test here but are predicted by PMT to have direct influence on individual protection motivation would be examined in our next step of the study. It might help us better understand why some of those outcome measures reported in this study fail to demonstrate the impact of PMT driven approach. Additional variables such as user experience and knowledge should also be considered as an experienced user can be indifference to our PMT manipulation.

Conclusion

This research aims to the development and effectiveness assessment of a theoretically sound training approach using protection motivation theory. This application of the protection motivation theory should provide new insights to researcher and practitioners who are interested in improving security training effectiveness. The current report is just a research in progress. With more comprehensive tests (including pretests) and evaluations being conducted and a full development of PMT driven hands on training modules, we expected our research can provide the foundations for a more general security awareness education model to be constructed. The PMT driven security exercise described here could be easily tailored to a variety of information security awareness training classes. Should the PMT driven approach prove to provide positive influence to security training outcomes, more training modules focusing on other topics of information security awareness can be designed and implemented.

REFERENCES

Alavi, M. and Leidner, Dorothy E. 1994. "Computer-mediated collaborative learning: An empirical evaluation." *MIS Quarterly* (18:2), pp. 159–174.

Ariyapperuma, S., &Minhas, A. 2005. "Internet security games as a pedagogic tool for teaching network security," In Frontiers in Education, 2005. FIE'05. *Proceedings 35th Annual Conference*, IEEE, pp. S2D-1

Baltzan, Paige. 2011, *Business Driven Information Systems, 3rd*, McGraw-Hill/Irwin

Cone, Benjamin D., Irvine, Cynthia E., Thompson, Michael F., Nguyen, Thuy D. 2007. "A video game for cyber security training and awareness," *Computers & Security* (26), pp. 63-72

Colquitt, Jason A. and Simmering, Marcia J. 1998. "Conscientiousness, Goal Orientation, and Motivation to Learn During the Learning Process: A Longitudinal Study," *Journal of Applied Psychology* (83:4)

Du, W., Wang, R. 2008. "SEED: A Suite of Instructional Laboratories for Computer Security Education." *ACM Journal on Educational Resources in Computing* (8:1)

Herath, Tejaswini and Rao, H.R. 2009. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, (47) pp. 154-165

Hill, J., Carver Jr, C. A., Humphries, J. W., & Pooch, U. W. 2001. "Using an isolated network laboratory to teach advanced networks and security," *ACM SIGCSE Bulletin* (33:1), pp. 36-40.

James E. Maddux and Ronald W. Rogers. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," Journal of Experimental Social Psychology (19), pp. 469-479

Klein, Howard J., Noe, Raymond A., Wang, Chongwei. 2006. "Motivation to learn and course outcomes: The impact of delivery mode, learning goal orientation, and perceived barriers and enablers," *Personnel Psychology* (59), pp. 665-702

Kroenke, David. 2013. *Using MIS 2013*, Prentice Hall

Kraiger, K., Ford, J.K., and Salas, E. 1993, "Application of cognitive, skill-based, and affective theories of learning outcomes to new methods of training evaluation," *Journal of Applied Psychology* (78:2), pp. 311–328

Lee,S.L. and Carter, G. 1972. A sample survey of departments of electrical engineering to determine

Locasto, M. E., & Sinclair, S. 2009. "An Experience Report on Undergraduate Cyber-Security Education and Outreach," in *Annual Conference on Education in Information Security (ACEIS)*

Logan, P. Y., & Clarkson, A. 2005. "Teaching students to hack: curriculum issues in information security," *ACM SIGCSE Bulletin* (37:1), pp. 157-161

MA, J. and J. V. Nickerson 2006. "Hands-On, Simulated, and Remote Laboratories: A Comparative Literature Review." *ACM Computing Surveys* (38:3)

Maughan, Douglas. 2010. "The need for a national cybersecurity research and development agenda," *Communications of ACM* (53:2), pp. 29-31

Meiselwitz, G. 2008. "Information Security across Disciplines," in *Proceedings of SIGITE'08*, October 16-18, 2008, Cincinnati, Ohio, USA.

National Institute of Standards and Technology. 2002. "Building an Information Technology Security Awareness and Training Program"

Riskowski, J. L., et al. 2009. "Exploring the Effectiveness of an Interdisciplinary Water Resources Engineering Module in an Eighth Grade Science Course," *International journal of engineering education* (25:1), pp. 181.

Rogers, R. W. 1975. "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology* (91), pp. 93-114

Schembari, N. P. 2007. "Hands-On Crypto': Experiential Learning in Cryptography," in *Proceedings of the 11th Colloquium for Information Systems Security Education*, pp. 7-13.

Schou, Corey D. and Trimmer, Kenneth J., 2004, "Information Assurance and Security," *Journal of Organizational and End User Computing on Information Security,* Editorial Preface

Shumba, R. 2004. "Towards a More Effective Way of Teaching a Cybersecurity Basics Course," *The SIGCSE Bulletin*, (36:4), pp. 108-111

Sommers, Kay and Robinson, Barbara. 2004. "Security awareness training for students at virginia commonwealth university," in *Proceedings of the 32nd annual ACM SIGUCCS* fall conference, pp. 379-380

Stair, Ralph M. and Reynolds George, 2012, *Fundamentals of Information Systems, 6th*, Cengage Learning

Vigna, G. 2003. "Teaching Hands-On Network Securty: Testbeds and Live Exercises," *Journal of Information Warfare* (2:3), pp.8-24.

Wan, Zeying, Compeau, Deborah, and Haggerty, Nicole. 2012. "The Effects of Self-Regulated Learning Processes on E‐Learning Outcomes in Organizational Settings," *Journal of Management Information Systems* (29:1), pp. 307–339

Weber, James E., Guster, Dennis, Safonov, Paul, and Schmidt, Mark B. 2008. "Weak password security: an empirical study," *Information security journal: a global perspective* (17) pp.45-54.