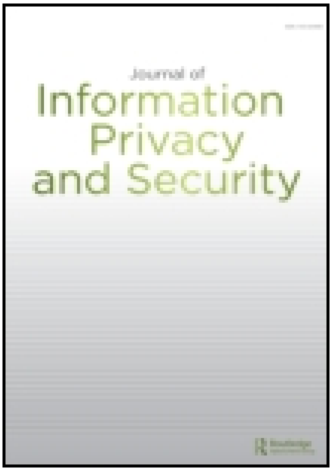


Journal of Information Privacy and Security
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uips20

Applying Protection Motivation Theory to Information Security Training for College Students

Peter Meso[a], Yi Ding[b] & Shuting Xu[c]

[a] Georgia Gwinnett College,

[b] Georgia Gwinnett College,

[c] Georgia Gwinnett College,

Published online: 07 Jul 2014.

To cite this article: Peter Meso, Yi Ding & Shuting Xu (2013) Applying Protection Motivation Theory to Information Security Training for College Students, Journal of Information Privacy and Security, 9:1, 47-67, DOI: 10.1080/15536548.2013.10845672

To link to this article: http://dx.doi.org/10.1080/15536548.2013.10845672

Applying Protection Motivation Theory to Information Security Training for College Students

Peter Meso, Georgia Gwinnett College, pmeso@ggc.edu

Yi Ding, Georgia Gwinnett College, yding@ggc.edu

Shuting Xu, Georgia Gwinnett College, sxu@ggc.edu

ABSTRACT

As Internet and Web technologies have been used in different fields by various organizations, cyber security has become a significant public concern for the society as a whole. There is a broad consensus on the need for broader and better training and education of the current and future workforce to be able to effectively deal with present, emergent and future cyber security challenges. However, cyber-security education tends to be constrained to computer and information science degree programs. Further, the courses within these programs tend to be offered via conventional instructional mechanisms that entail limited hands-on learning experiences due to the difficulty, cost, and potential risks of setting up real world like hands-on security training environments, which are often network-based.

Considering cyber security education is a necessary need across all disciplines and majors, we have been undertaking a research project at a public college to (a) construct a model to study the influence of knowledge from lectures and hands-on experience on security behavior using protection motivation theory (b) develop a series of laboratory based Information Security education modules as easy to tailor and scalable pedagogic tools for helping undergraduate students to comprehend information security at different levels , and (c) test the impact of these modules on students' post-training personal cyber security behavior. Our aim is to identify if indeed students do apply what they learn to confidently and intelligently address personal cyber security challenges, after they have completed these course modules. In this paper, we report (a) our theoretical model (b) the design of security pedagogy modules and, (c) the preliminary findings upon testing and surveying students' post-training knowledge and post-training behavior concerning the security topics covered in the training modules.

INTRODUCTION

Organizations are increasingly using and depending on the Internet and Web services to reach and serve customers as well as organize and manage business activities. Consequently, their needs to protect corporate information systems and assets from various cyber threats that might cause financial losses and damage in business reputation are also increasing. The recent Bloomberg Business Week report of cyber attack on U.S. bank systems (Strohm and Engleman, 2012) just reminds us how real those cyber threats can be and how serious the troubles they can make on our daily life and businesses. The ability to address information security concerns and challenges is crucial to today's nomadic-computing-prone workforce. Therefore, "understanding these threats and identifying high-level solutions to protecting the organization are essential capabilities" (Topi, H., J. S. Valacich, et al. 2010, p. 377) for college-graduates today, regardless of their areas of specialization.

Since the breach of system security often happens at the weakest point of a system, the scope of information systems security should cover the whole system, which consists of not only just technology components, such as hardware, software, and data but also managerial components, such as procedures, policies, and people. According to the Association for Computing Machinery (ACM) Information Technology (IT) 2008 Curriculum Guideline, information security is a pervasive theme, which should span across all the other areas of the IT curriculum (Lunt et al. 2008). The guidelines further state that educating students in information security is most effective when the subject is "addressed multiple times in multiple classes, beginning in the IT fundamentals class and woven like threads throughout the tapestry of the IT curriculum" (Lunt et al. 2008, p. 33). To understand how pervasive the information security theme is through IT related curriculum we used IT courses offered at our current institution as a sample base and found that over 30% of those courses listed some information security related topics as part of their key learning objectives. Those courses represent a broad spectrum of information systems education at various levels - from very fundamental levels with audience who are mainly non-IT majors to the advanced level with audience who are mainly IT major students. Although many of those courses share overlapping information security themes, we found that there is a lack of systematic and coherent approach to provide students consistent quality learning experiences pertaining to cyber security across the IT curriculum. In some courses (particularly, in those lower level IT courses), information security topics are delivered in a pure lecturing style without any hands-on exercises. In other courses, hands-on lab modules covering overlapping security topics are often developed independently. There is a lack of consideration of how those modules might be chained or organized together in a way that allows them to supplement each other and to help students develop an in-depth understanding of information security concepts to the point that they routinely apply that knowledge in their daily use of information systems.

This paper reports our first phase findings from a multi-phase initiative that seeks to develop a scalable information systems security education handbook for use across multiple disciplines and multiple levels of education within a four-year liberal arts education institution. Ultimately, we hope this handbook can deliver consistent hands-on learning experience of information security concepts across all levels in both the IT curriculum, and the curriculum of non-IT disciplines because computer literacy in today's world "emphasizes knowledge combined with practical, hands-on expertise"

(Lunt et al. 2008, p. 19). If successful, our experience and findings could greatly benefit other similar educational institutions having similar security education needs. In this study we specifically compare the influence of information security knowledge garnered from lectures-only courses with that garnered from courses emphasizing hands-on projects, on student's post-training security behavior. To do this, we constructed a theoretical model using the protection motivation theory (PMT) and used it to examine and explain observed differences across students in these two kinds of courses. We are particularly interested in identifying how the two approaches to delivering systems security education contributed to students' threat appraisals and the coping appraisals as operationalized in PMT, and how these two constructs influence the students' intensions for security actions.

The remainder of the paper will proceed as follows. First, a summative review of the literature on pedagogical instruments adopted in information security education and the protection motivation theory as applied in information security behavior is presented. Next we present the motivation for this study. We then present the research model, hypotheses and research methodology. Finally, we wrap up the paper with conclusions and an articulation of potential future work.

LITERAURE REVIEW

Many IT or Information Systems (IS) literacy textbooks often include information security as a major subject (e.g., Baltzan 2012; Kroenke 2012; Stair and Reynold 2012). Plentiful information security concepts such as malware, identity theft, password cracking, firewall, denial of service, wireless security, etc. are covered in these kinds of courses. Typically, those concepts along with suggested practices to maintain good security are taught with traditional lecturing that relies on "textbooks, slides, papers" and student performance of learning those concepts is often evaluated with "paper-based and theoretical" assignments or tests (Vigna 2003, p. 8). The discussions of those concepts in class often focus on facts and description of concepts or some case studies. As concepts such as malware, password cracking, hacking, etc. are technical oriented researchers argue traditional lecturing often leaves "students with little understanding of application of concepts" in a real-world scenario (Riskowski et al., p. 182). This could also limit their appreciation of suggested good security practices to battle with cyber threats, as they can hardly comprehend the severity of those threats that might be caused by malpractice in their day-to-day use of IT.

Hands-on approach has been promoted by a number of researchers in the fields of science and technology as a key tool for achieving effective learning of scientific and technological subjects (MA and Nickerson 2006). In the information security field, numerous hands-on based labs and projects have been proposed and discussed for education purpose (e.g., Logan and Clarkson 2005; Hill et al. 2001; Ariyapperuma & Minhas 2005; Schembari 2007; Locasto & Sinclair 2009, etc.). Most of those hands-on exercises are developed for students majoring in IT to study information security topics at an advanced level. Therefore, while it is evident that numerous pedagogical instruments (e.g., labs, tools, simulation methods, etc.) have been developed to provide students with hands on IT educational experiences (Du and Wang 2008, Shumba 2004, Stevenson and Romney 2004), few studies have discussed how those pedagogical instruments might be applied to teaching cyber security concepts within non IT courses or IT courses with a significant portion of non IT majors (Meiselwitz 2008; Slusky and Partow-Navid, 2012). Most of the hands-on tools for systems security education proposed and developed in the literature tend to be integrative in nature and often require that students already exhibit a solid IT foundation knowledge in order to understand, complete and benefit from them.

One of the key questions asked by MA and Nickerson (2006) in their review of laboratory approaches applied in scientific education "Can technology promote students' learning or not" can be rephrased and asked here in the field of information security education as "Can hands-on exercises promote students' learn or not?" To answer this question, an effective evaluation tool is needed. In the current information security education domain most of existing studies applying hands on approaches in education tend to focus on the design and development of those approaches instead of evaluating them. The evaluation part tends to be brief, ad-hoc, and mostly based on self-reported qualitative feedback from students. This phenomena is also consistent with MA and Nickerson's (2006) observation in science and engineering education that there are no standard criteria to evaluate the effectiveness of hands-on pedagogical components. Researchers have argued that clear and well-formed objectives are needed for effective evaluation of hands-on learning initiatives (Lee and Carter 1972). In our study we not only focus on the development of hands-on modules but also recognize the need of effective evaluation of those modules.

MOTIVATION

Today, all college-level students extensively use cyber-based instructional technologies such as course management systems (Boettcher 2003, Carmean and Haefner 2002, Malikiwski et al. 2007) and operate in an environment that expects them to be acquainted with and competent at optimizing their personal security when using internet-based information systems (Walden 2008, Wang 2005). Studies on information systems pedagogy also echo an unintended bias concerning systems security education. For one, systems security concepts tend to be rather technical and complex. Because of this they tend to be covered in advanced IT courses, which are largely the preserve of IT majors. Consequently, non-IT majors particularly suffer from an inadequate exposure and coverage of information security concepts. Further, teaching these concepts to non-IT majors, most of whom may lack a fundamental grounding in IT knowledge is challenging, especially where conventional approaches to teaching systems security are adhered to. Secondly, emphasis on systems security pedagogy tends to be on the information system – the technological artifact, with topics focusing on strategies and approaches to securing the system, technological algorithms and tools for cryptography and network-data management, and the establishment of perimeter defense mechanisms, among others. Topics pertaining to personal security when using networked-systems, individual's responsibility in secure-use of information systems, and significance of knowledgeable application of security-optimizing behavior when using information systems tend to be less emphasized. Further, these latter concepts are rarely delivered via hand-on lab approached. Rather, the lecture of case-based approaches seem to be preferred as the pedagogical approaches to addressing behavioral issues of information security.

Hence the motivation for this study: How can we extend effective systems security education to all students at a four year undergraduate liberal arts university such that all become deeply knowledgeable of information security concepts as to alter their system use behavior? This is particularly challenging given that a significant proportion of systems security concepts are very technical, integrative and often require students to have a solid foundation IT knowledge prior to studying those information security concepts. Hence teaching systems security to non-IT students, most who might be lacking solid foundational IT knowledge, could be quite challenging.

A preliminary online survey that we conducted to measure the information security awareness and behavior of our students before and after they learned the security material was completed by 77 students registered in 7 sections of a first-year college information technology course taught by 4 different faculty members. The survey reveals that after students had completed the course-module on computer and systems security through regular classroom lectures, their awareness of security attacks increased by 28% and their awareness of malware increased by 11% (Figure 1). However, their confidence and skills in dealing with these security issues only increased by 8%. But this was not as bad as the observed change in their security related behaviors, which improved by a paltry 4%.

The survey results show that whereas students' knowledge pertaining to information security issues was noticeably expanded, their skills and behavior on security issues was not improved as expected. Thus we were motivated begin to examine the theory-based reasons for this observation and also to question if the development of hands-on projects for training student on these issues would leverage their skills and strengthen their confidence in dealing with information security issues. We settled on the PMP as the theory base for our study and the comparison of the lecture-based pedagogical approach to the hands-on lab based pedagogical approach as the primary thrust of the study. The objective of the study is to identify if hands-on labs result in deeper-learning, the kind of which would significantly improve student's post-training systems security behaviors. The rest of this paper outlines the PMP as it applies to this study, and consequently, documents the study's hypotheses, research design, and findings.

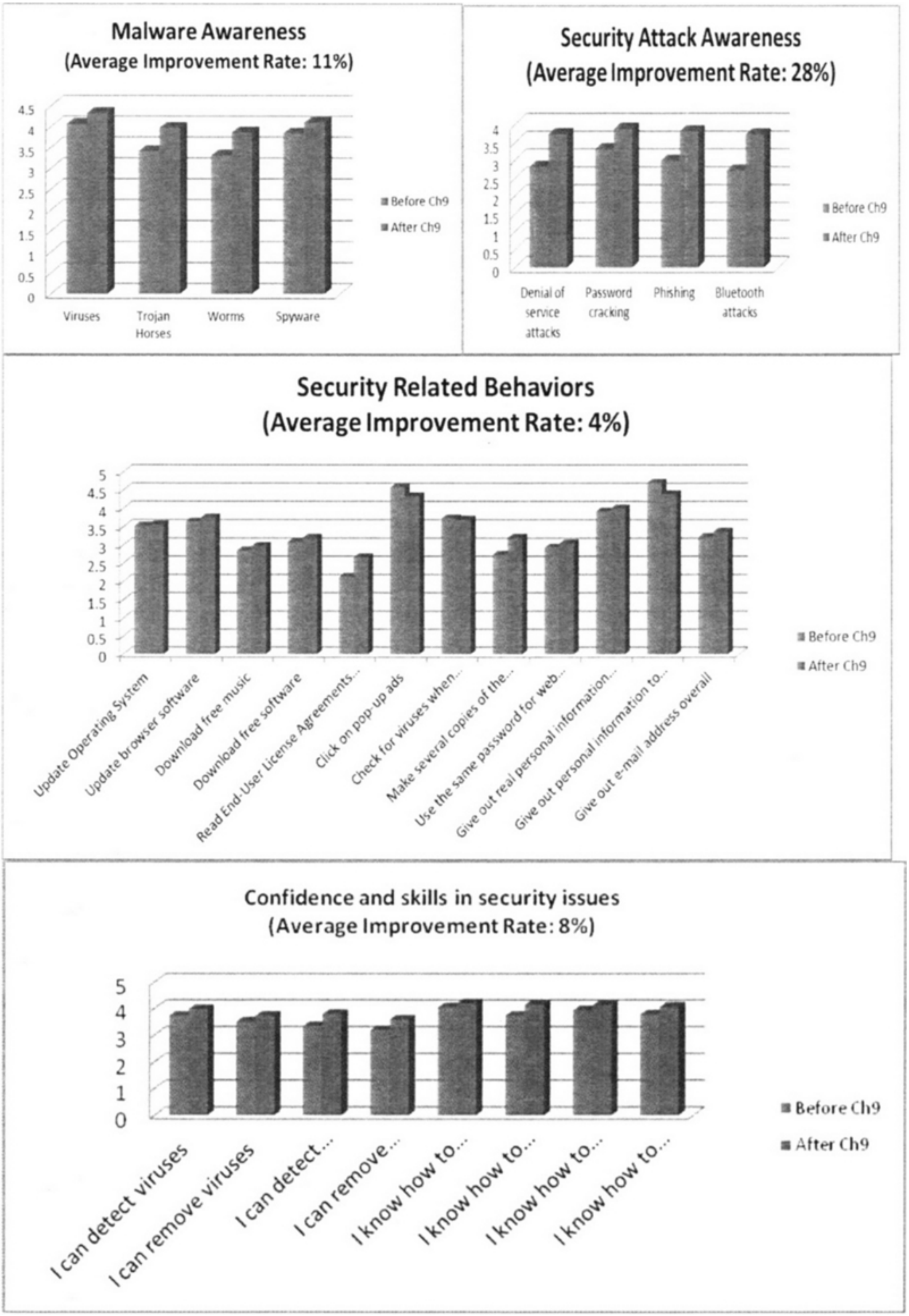


Figure 1. Preliminary survey results

RESEARCH MODEL AND HYPOTHESES

Protection Motivation Theory

The protection motivation theory (PMT) was originally founded by Dr. R.W. Rogers in 1975 in order to better understand fear appeals and how people cope with them (Rogers 1975). PMT has been noted as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson and Agarwal, 2010). Protection motivation stems from both the threat appraisal and the coping appraisal. The threat appraisal assesses the severity of the situation and examines how serious the situation is. The coping appraisal is how one responds to the situation. The threat and coping appraisal variables combine in a fairly straightforward way, although the relative emphasis may vary from topic to topic and with target population.

The threat appraisal process consists of both the severity and vulnerability of situation. It focuses on the source of the threat and factors that increase or decrease likelihood of maladaptive behaviors (Plotnikoff and Ronald, 2010). The total amount of threat experienced is the sum of the perceived severity and perceived vulnerability.

Perceived vulnerability (PV) refers to an individual's assessment of the probability of threatening events. In this paper, it refers to the students' assessment of the probability of security breaches.

Perceived severity (PS) refers to the severity of the consequences of the event. In this paper, it refers to the students' assessment of the severity of security breaches.

The coping appraisal consists of the response efficacy, self-efficacy, and the response costs. It refers to an individual's assessment of his or her ability to cope with and avert the potential loss or damage arising from the threat (Woon et al., 2005). The amount of coping ability that one experiences is the combination of response efficacy and self-efficacy, minus the response costs.

Response efficacy (RE) is the effectiveness of the recommended behavior in removing or preventing possible harm. In this paper, it refers to the students' assessment of various security protection methods and software.

Self-efficacy (SE) is the belief that one can successfully enact the recommended behavior. In this paper, it refers to the students' ability to apply appropriate methods and software to protect security.

Response costs (RC) are the costs associated with the recommended behavior. In this paper, it refers to the monetary, time, and efforts expended in applying appropriate methods and software to protect security.

Research Model

The research model is presented in Figure 2. Behavioral intent is directly influenced by perceived severity and perceived vulnerability from the threat appraisal, and response efficacy, self-efficacy, and response costs from the coping appraisal. Knowledge from lectures (KL) influences perceived severity, perceived vulnerability, response efficacy and self-efficacy. Experience from hands-on projects (EH) influences the same four constituents and besides that, it also influences response cost.

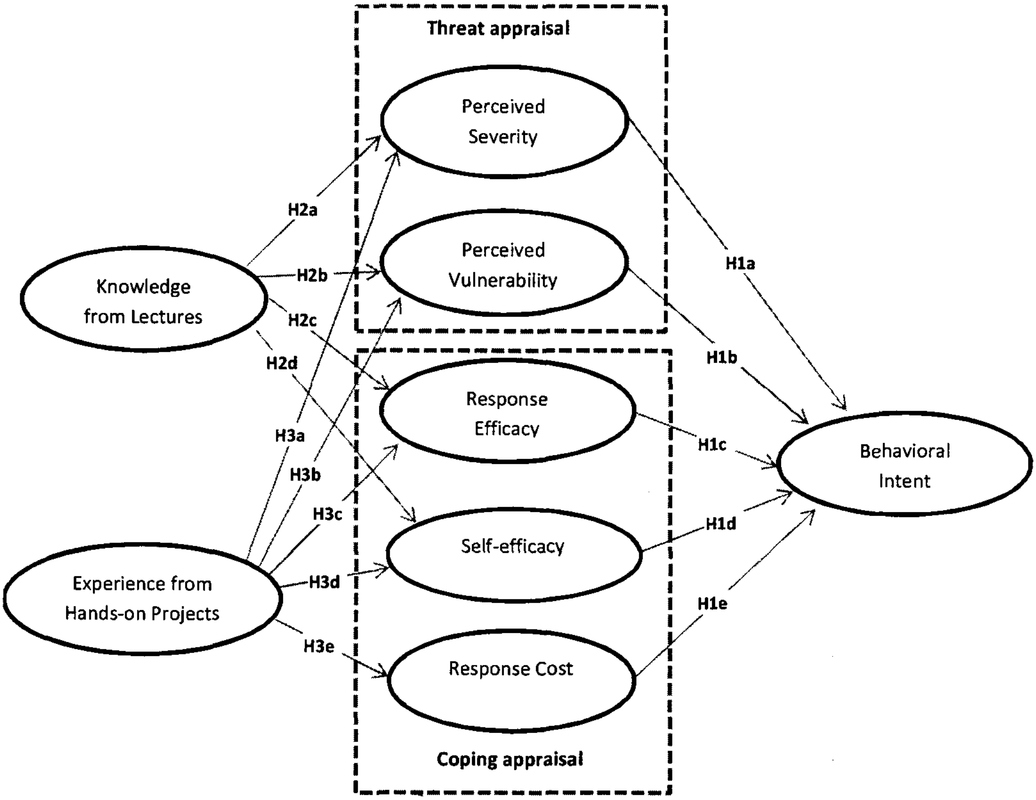


Figure 2. Research model

Hypotheses Development

The protection motivation theory suggests that information about a threat causes a cognitive mediating process in individuals that appraises positive or negative responses (Vance, Siponen and Pahnila, 2012). Thus students' adoption of information security methods and software represents an adaptive response, while non-adoption is a maladaptive response. Vulnerability is to the probability thatan unwanted incident will happen if no actions are taken to prevent it. In our study, vulnerability denotes students' assessment of whether their computers and personal information is open to security threats if no measures are taken to prevent them. It is reasonable to expect that a student who perceives high vulnerability to his or her IS resource will be more likely to adopt protective behaviors. Severity, is the level of the potential impact of the threat. In our context, it refers to the severity of the IS security breach, and the possible negative influences caused by the breach. According to Pechmann et al. (Pechmann et al., 2003), an individual's perceived severity tends to be positively linked to their intentions to follow protective actions. Hence, we hypothesized the following:

H1a: *Perceived severity will have a positive effect on student intentions to adopt appropriate information security actions.*

H1b: *Perceived vulnerability will have a positive effect on student intentions to adopt appropriate information security actions.*

Response efficacy represents the scenario when an individual possesses requisite knowledge about the effectiveness of a recommended coping mechanism in providing protection from a threat or danger, the individual is more likely to adopt an adaptive behavior (Woon et al., 2005). Thus, a student's response efficacy tends to be positively linked to his or her intention to adopt information security actions. Self-efficacy has been shown to have a significant impact on an individual's ability to accomplish task behavior, including IS usage (Compeau and Higgins, 1995). Compeau and Higgins (1995) showed that people with higher levels of self-efficacy regarding IS use will employ such systems in their work more than those with low self-efficacy. Hence, we hypothesized:

H1c: *Response efficacy will have a positive effect on student intentions to adopt appropriate information security actions.*

H1d: *Self-efficacy will have a positive effect on student intentions to adopt appropriate information security actions.*

Response costs may include monetary expense, timing inconveniences, embarrassment or other negative consequences (Pahnila et al. 2007). According to Lee and Larsen (Lee and Larsen, 2009), individuals are reticent to follow or adopt recommended responses if they perceive that a considerable amount of resource i.e. time, effort, and money will be expended toward an effort. They have also shown that response costs is negatively related to intention to adopt security measures.

H1e: *Response cost will have a negative effect on student intentions to adopt appropriate information security actions.*

Knowledge from lectures will enable students to more accurately assess the vulnerability of their computers and the severity of security breaches. Students can get knowledge on security protection methods and software, thus it will positively influence response efficacy. Knowledge may also improve students' ability to apply appropriate methods and software to protect security. Hence, we hypothesized:

H2a: *Knowledge from lectures will positively influence perceived severity.*

H2b: *Knowledge from lectures will positively influence perceived vulnerability.*

H2c: Knowledge from lectures will positively influence perceptions of response efficacy.
H2d: Knowledge from lectures will positively influence perceptions of self-efficacy.

The original formulation of PMT explicitly suggested that ''prior experience'' was a preceding factor for PMT (Vance, Siponen and Pahnila, 2012). Thus, we posit that experience from hands-on projects has a negative influence on response cost and a positive influence on all the other constructs of PMT. Hence, we hypothesized:
H3a: Experience from hands-on projects will positively influence perceived severity.
H3b: Experience from hands-on projects will positively influence perceived vulnerability.
H3c: Experience from hands-on projects will positively influence perceptions of response efficacy.
H3d: Experience from hands-on projects will positively influence perceptions of self-efficacy.
H3e: Experience from hands-on projects will negatively influence response cost.

RESEARCH METHODOLOGY

Data Collection

This research used an internet-based survey to collect data from respondents. The survey questions were adapted from previous research (Anderson and Agarwal, 2010, Johnston and Warkentin, 2010) but re-written to fit the context within which the study was being conducted. Table 1 presents the survey questions. Respondents were drawn from college students at Georgia Gwinnett College enrolled in the Introduction to Computing course. The survey was conducted after students learn the chapters covering information security. Students were divided into two groups. One group of students worked on the hands-on projects for a week besides the classroom lectures and another group only had classroom lectures. Ensuing is a brief description of each of the hands-on projects employed in this study.

Hands-on Projects Implementation

The Introduction to Computing course is a general education course that is required for all college students to take regardless their majors. One of its major learning goals focuses on helping students acquire basic knowledge of computer security, protection mechanisms and privacy threats on the Internet. This course also includes a dedicated chapter covering a variety of information security related topics including cybercrime, viruses, physical and online digital assets protection, online annoyances, social engineering, and data backup. To help those non-IT major students better understand those topics, we adopted and customized two hands-on projects: password-cracking project and virus analysis project, which are typically designed for IT major students to study those subjects at an advanced level, given the time limitation (one week class) and student knowledge limitation (as many of them lack solid IT knowledge and skills). These modules are described below.

Password-cracking Project

Hackers trying to gain unauthorized access to any system often try to acquire the usernames and passwords of legitimate users. Good information security starts with following good password security practices in user account creation, then doing regular checks for the integrity of password files (Shumba 2004). This project introduces students to different ways of creating user accounts and how to check for the integrity of password files using password cracking programs such as John the Ripper (http://www.openwall.com/john/). Students will create password using a) a dictionary word, b) a commonly used word, c) the same as username, d) repeating characters, e) has both uppercase and lowercase characters, and f) a combination of lowercase characters, uppercase characters, and numbers. After account creation, students then use John the Ripper to identify weak passwords. Upon completion of this exercise students are able to understand the importance of following good security practices in user account creation.

Virus Analysis Project

Virus is an important topic in information security. This project shows students the destructive feature of virus and ways to eliminate them. Students will download files infected by different types of virus and observe the destruction they may cause. Then students will remove the virus using a) anti-virus software b) manually following the instructions found on the anti-virus web site. Students will compare the effectiveness of the two ways in identifying and repairing infections. Upon completion of this exercise students are able to understand the severity of the virus attacks and the importance of installing and updating anti-virus software.

Table 1. Survey-instrument items mapped to respective constructs in the theoretical model

Construct	Construct Source	Measurement Items (Questions)
Perceived vulnerability	Anderson and Agarwal, 2010, Johnston and Warkentin, 2010	1. My passwords are at risk of being hacked. 2. It is likely that my password will be hacked. 3. My computer is at risk of becoming infected by viruses. 4. It is likely that my computer will become infected by viruses.
Perceived severity	Anderson and Agarwal, 2010, Johnston and Warkentin, 2010	1. If my password were hacked, it would be severe. 2. If my computer were infected by viruses, it would be severe.
Response efficacy	Anderson and Agarwal, 2010, Johnston and	1. Using a strong password will reduce the possibility that it will be hacked. 2. Anti-virus software is effective in removing the viruses.

	Warkentin, 2010	
Self-efficacy	Anderson and Agarwal, 2010, Johnston and Warkentin, 2010	1. I know how to create a strong password. 2. I know how to remove viruses from my computer. 3. I know how to remove viruses if anti-virus software does not work. 4. I know how to crack a password.
Response costs	Anderson and Agarwal, 2010, Johnston and Warkentin, 2010	1. It takes me a lot of time to create a strong password. 2. It takes a lot of effort to create a strong password. 3. It takes a lot of effort to remove viruses from my computer. 4. It takes me some time to install and use anti-virus software. 5. It takes a lot of time to remove viruses.
Behavioral Intent	Anderson and Agarwal, 2010, Johnston and Warkentin, 2010	1. The next time I am asked to create a new password, I will create a simple password. 2. I use very simple passwords such as dictionary words, people's names, or numbers like 123456. 3. The next time I am asked to create a password, I will use a composition of lower case letters, upper case letters, numbers, and/or special characters. 4. If my computer becomes infected by viruses, I will use anti-virus software to remove them.
Knowledge from Lectures (only for post-chapter survey)	Anderson and Agarwal, 2010, Johnston and Warkentin, 2010	1. Lectures are helpful for me to learn how to create a strong password 2. Lectures are helpful for me to understand the harmful features of viruses. 3. Lectures are helpful for me to learn how to remove viruses if my computer were infected.
Experience from Hands-on Projects (only for students working on the projects)	Anderson and Agarwal, 2010, Johnston and Warkentin, 2010	1. Hands-on projects are helpful for me to learn how to create a strong password. 2. Hands-on projects are helpful for me to understand the harmful features of viruses. 3. Hands-on projects are helpful for me to learn how to remove viruses if my computer were infected.
Demographic Information	N/A	1. Gender 2. Major (Which school)
Computer Background	N/A	1. Do you have a computer? 2. Do you use Internet every day? 3. How long on average do you use computer every day?

EMPIRICAL ANALYSIS AND RESULTS

Descriptive Statistics

All the respondents were college students enrolled in an introductory information technology course at Georgia Gwinnett College. Among the respondents, the male to female ratio was approximately 3:2. Survey data reflected that 91% of the respondents owned a computer and 86% of them used the Internet every day. For the time spent on computer, 47% of the respondents used computers 1-3 hours a day and 34% of the respondents used computers 4-5 hours a day. There were also 16% of the respondents who used computer more than 6 hours a day.

Assessment of the Theoretical Model

In order to empirically test our research model, we used the Partial Least Squares (PLS) method as implemented in SMART PLS software (Ringle, 2005). Data collected via the survey instrument was executed in Smart PLS. This allowed us to validate the survey instrument and also to test the study's hypotheses. We report the results of this analysis in this section. First we articulate our findings concerning assessment of the survey instrument, termed assessment of the measurement model within PLS discourse. Then we report our findings about the testing of structural model, i.e. the hypotheses testing.

Assessment of the Measurement Model

The measurement model tests provide validity indicators pertaining to the survey instrument. We tested the survey instrument's reliability, construct validity, convergent validity, and discriminant validity. Cronbach's alpha values were used to assess the instrument's reliability (Nunnally, 1967). All of the Cronbach's alpha values, except that for response efficacy, were above 0.70 (Table 2).

Table 2: Cronbach alpha and convergent validity statistics for model's constructs

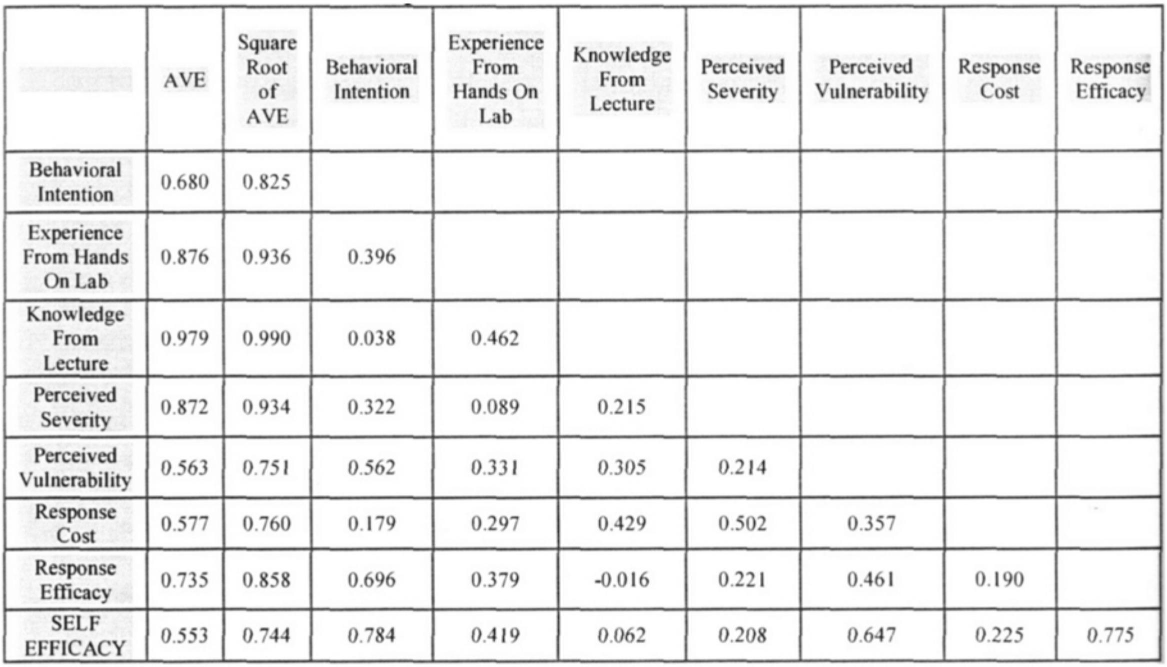
CONSTRUCT	RELIABILITY (Cronbach's Alpha)	CONVERGENT VALIDITY (Composite Reliability)
Behavioral Intention	0.767	0.864
Experience From Hands On Lab	0.953	0.966
Knowledge From Lecture	0.993	0.995
Perceived Severity	0.854	0.932
Perceived Vulnerability	0.742	0.837
Response Cost	0.764	0.845
Response Efficacy	0.662	0.847
Self Efficacy	0.730	0.830

Construct validity assesses how item loading on their respective constructs. We tested construct validity by way of confirmatory factor analysis (CFA). Table 2 provides the results of this test. We concluded that all of the original items (listed in Table 1) loaded adequately because each had a value greater than 0.60 (Gefen, 2000).

The constructs in the model were also found to have adequate convergent validity. According to Nunnally (1967, 1978), convergent validity is adequate when the rank correlation coefficient (rho) value of each construct as determined by the respective loading of the items is greater than 0.70. As is evident in Table 2, all constructs have a rho-value greater than 0.70.

We used two approaches to assess discriminant validity. First, we examined the correlations among the constructs and their respective indicators to establish that each indicator had a higher correlation with its respective construct that it did with the other constructs in the theoretical model. This was found to be the case. Second, we used the square root of the average variance extracted (AVE) of each construct and contrasted that to the correlations of that construct to the other constructs in the model. Table 3 presents the results of this analysis. We found that the square root of the AVE was higher than respective correlations for each construct in the theoretical model. Therefore, we concluded that all the constructs in the theoretical model demonstrated satisfactory discriminant validity.

Table 3. AVE, square root of AVE and construct correlations



	AVE	Square Root of AVE	Behavioral Intention	Experience From Hands On Lab	Knowledge From Lecture	Perceived Severity	Perceived Vulnerability	Response Cost	Response Efficacy
Behavioral Intention	0.680	0.825							
Experience From Hands On Lab	0.876	0.936	0.396						
Knowledge From Lecture	0.979	0.990	0.038	0.462					
Perceived Severity	0.872	0.934	0.322	0.089	0.215				
Perceived Vulnerability	0.563	0.751	0.562	0.331	0.305	0.214			
Response Cost	0.577	0.760	0.179	0.297	0.429	0.502	0.357		
Response Efficacy	0.735	0.858	0.696	0.379	-0.016	0.221	0.461	0.190	
SELF EFFICACY	0.553	0.744	0.784	0.419	0.062	0.208	0.647	0.225	0.775

Assessment of the Structural Model

In PLS, the structural model is used to assess a study's hypotheses and R^2 values. Since each path within the structural model represents a specific hypothesis the path coefficient becomes a measure of support or disproval of the hypothesis. The R^2

values represent the amount of variance explained by independent variables. The R^2 values are presented in Figure 2 for each dependent variable.

Results of the assessment of the hypotheses as operationalized in the structural model are indicated in Figure 2 and summarized in table 4. Borrowing from prior research in the information sciences, we hold the criteria for determining whether or not a hypothesis is ``supported'' to be strictly path coefficients greater than 0.20 and having a p-value that is less or equal to 0.05. Based on these criteria, seven out of the fourteen hypotheses were significantly supported; three hypotheses–H1e, H2a, and H2b – showed weak support; while, four hypotheses – H1b, H2c, H2d and H3a – were not supported.

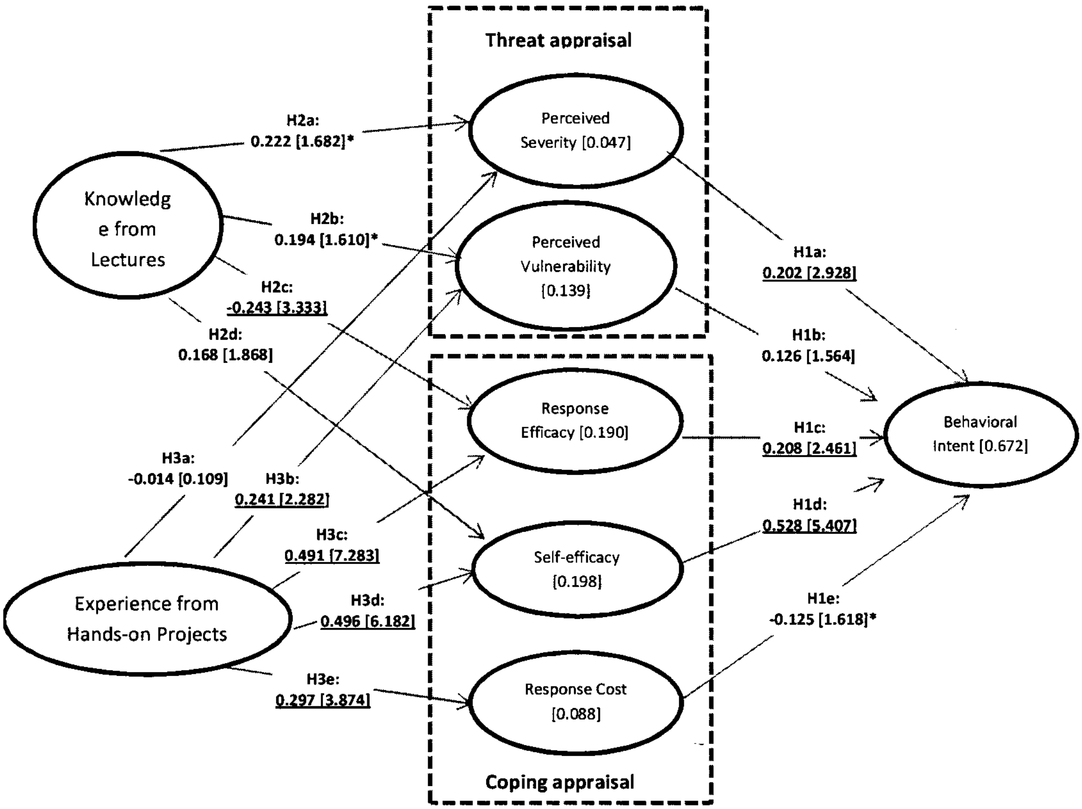


Figure 3. Graphical representation of study's results

Legend

Hypothesis Not Supported: Path-Coefficient [T-Value],

Hypothesis Partially Supported: Path-Coefficient [T-Value]*

Hypothesis Fully Supported: Path-Coefficient [T-Value]

Table 4: Results of hypothesis testing

SPECIFIC HYPOTHESIS	PATH COEFFICIENT	T-VALUE	RESULT
▪*H1a: Perceived severity will have a positive effect on student intentions to adopt appropriate information security actions.*	0.202	2.928	SUPPORTED
▪*H1b: Perceived vulnerability will have a positive effect on student intentions to adopt appropriate information security actions.*	0.126	1.564	NOT
▪*H1c: Response efficacy will have a positive effect on student intentions to adopt appropriate information security actions.*	0.208	2.461	SUPPORTED
▪*H1d: Self-efficacy will have a positive effect on student intentions to adopt appropriate information security actions.*	0.528	5.407	SUPPORTED
▪*H1e: Response cost will have a negative effect on student intentions to adopt appropriate information security actions.*	-0.125	1.618	MARGINAL
▪*H2a: Knowledge from lectures will positively influence perceived severity.*	0.222	1.682	MARGINAL
▪*H2b: Knowledge from lectures will positively influence perceived vulnerability.*	0.194	1.610	MARGINAL
▪*H2c: Knowledge from lectures will positively influence perceptions of response efficacy.*	-0.243	3.333	NOT SUPPORTED
▪*H2d: Knowledge from lectures will positively influence perceptions of self-efficacy.*	-0.168	1.868	NOT SUPPORTED
▪*H3a: Experience from hands-on projects will positively influence perceived severity.*	-0.014	0.109	NOT SUPPORTED
▪*H3b: Experience from hands-on projects will positively influence perceived vulnerability.*	0.241	2.282	SUPPORTED
▪*H3c: Experience from hands-on projects will positively influence perceptions of response efficacy.*	0.491	7.283	SUPPORTED
▪*H3d: Experience from hands-on projects will positively influence perceptions of self-efficacy.*	0.496	6.182	SUPPORTED
▪*H3e: Experience from hands-on projects will negatively influence response cost.*	0.297	3.874	SUPPORTED

In summary, the study reveals that while lecture-based approaches have value with respect to enhancing perceived students' post-training personal cyber security behavior, hands-on approaches seem to offer stronger effects.

Discussion

One of the main focus of this paper was to test whether PMT predicts a student's security behavior intention well. The findings show three out of five key PMT variables are significant predictors of a student's behavior intention. According to PMT, an individual's behavior intention is predicted by threat appraisal and coping appraisal variables. The threat appraisal variables are made up by the perceived severity and perceived vulnerability. This study supports perceived severity but not perceived vulnerability as a significant predictor of an individual's security behavior intention. However, this finding by no means disapproves the perceived vulnerability as an important security behavior predictor. Such a result might be caused by various reasons. It could be our sample size is too small to find the influence of perceived vulnerability. Or, it could be students are not capable of answering the perceived vulnerability related question due to their lack of experience. Specially, some students are light computer users and never own or maintain a computer by themselves. They might never have any security breach experience. In this case, even one dose of hands-on treatment might not be enough for them to appropriately assess vulnerability, which is defined as the probability of security breaches. The other PMT variable that is not supported or only marginally supported in this study is response cost. It is a coping appraisal variable. Again, this insignificant finding in this study cannot disapprove it as a key PMT variable. This result might also be caused by limited sample size or inexperienced students.

The other key objective was to examine the efficacy of two different pedagogical approaches to teaching systems security concepts: lecturing and hands-on exercise. We find a striking difference between these two. For one, all hypotheses related to how lecturing might influence PMT variables are not supported. On the other hand, almost all but one hypothesis related to how hands-on exercises influence PMT variables are supported. This might indicate hands-on exercises do promote students with greater ability to assess the severity of the situation and know how to respond to it. Such a result also supports our initiative in developing pedagogical tools that can deliver students hands-on experience.

Limitations

It is import to point out that our findings need further verification in future studies because this study is not without limitation. One limitation would be that our study does not examine the learning efficacy, which indicates how much content knowledge students acquired. An examination of this variable might help us better understand why lecturing has such little influence on those PMT variables. Maybe, it is caused by the way the lecture is organized. Another limitation, as mentioned earlier in this paper, is the sample size. More studies within larger groups of students located in different institutions could help reduce the possible biases in our study. In addition, the nature of cyber-security education modules employed in our current study, all of which were quite rudimentary in nature, could be another limitation of our study as our results show that there is still one hypothesis related to the influence of hands-on exercises that is not supported.

CONCLUSION AND FUTURE WORKS

This study sought to examine the influence of knowledge obtained from lectures and hands-on experience on security behavior using protection motivation theory. It employed the protection motivation theory to provide insights into the individual perceptions that lead to security adoption behavior, and how these are shaped by the type of instruction received. The proposed model, and specifically the construct "Experience from hands-on projects" proved to be a significant predictor of security behavior. In this regard, this study provides the foundation for advancing and promoting the use of lab-based hands-on approaches to information security training with a view to fostering appropriate long-term individual behavior pertaining to systems security.

REFERENCES

Anderson C. L., Agarwal R. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), 2010, pp. 613-43.

Ariyapperuma, S., & Minhas, A. "Internet Security Games as a Pedagogic Tool for Teaching Network Security," In Frontiers in Education, 2005. FIE'05. Proceedings 35th Annual Conference (pp. S2D-1). IEEE.

Baltzan, P. *Business Driven Technology*, McGraw-Hill, 2012.

Boettcher, J. V. Course Management Systems and Learning Principles: Getting To Know Each Other.... Syllabus, v16 n12 p33-34, 36 Jul 2003.

Carmean, C., and Haefner, J. "Transforming Course Management Systems into Effective Learning Environments," *Educause Review*, November/December 2002, pp. 27-34.

Strohm C., and Engleman E. "Cyber Attacks on U.S. Banks Expose Vulnerabilities, Bloomberg Businessweek, 28 September 2012, http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability

Compeau, D. R., and Higgins, C. A. "Computer Self-efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), 1995, pp. 189-211.

Du, W., and Wang, R. "SEED: A Suite of Instructional Laboratories for Computer Security Education," *ACM Journal on Educational Resources in Computing* (8:1.3), 2008.

Gefen D, Straub D, and Boudreau MC. "Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice," *Communications of the Association of Information Systems* (4), 2000, pp.1–70.

Hill, J., Carver Jr, C. A., Humphries, J. W., and Pooch, U. W. "Using an Isolated Network Laboratory to Teach Advanced Networks and Security," *ACM SIGCSE Bulletin* (33:1), 2001, pp. 36-40.

Johnston, A. C., Warkentin, M. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), 2010, pp. 549-566.

Kroenke, D. M. Using MIS, Pearson, 2012.

Lee,S.L., and Carter, G. "A Sample Survey of Departments of Electrical Engineering to Determine, 1972.

Lee, Y., and Larsen, K. R. "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-malware Aoftware," *European Journal of Information Systems* (18:2), 2009, pp. 177-187.

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

Logan, P. Y., and Clarkson, A. "Teaching Students to Hack: Curriculum Issues in Information Security," *ACM SIGCSE Bulletin* (37:1), 2005, pp. 157-161.

Lunt, B. M., J. J. Ekstrom, et al. Curriculum Guidelines for Undergraduate Degree Programs in Information Technology, Association for Computing Machinery (ACM) and IEEE Computer Society, 2008.

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

Malikiwski, S. R., Thompson, M. E.,and Theis, J. G. "A Model for Research into Course Management Systems: Bridging Technology and Learning Theory," *J. Educational Computing Research* (36:2), 2007, pp. 149-173.

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

Nunnally J. *Psychometric Theory*, 1st ed. New York: McGraw-Hill, 1967.

Nunnally J. *Psychometric Theory*, 2nd ed. New York: McGraw-Hill, 1978.

Pahnila, S., Siponen, M., and Mahomood, A. "Employees' Behavior Towards IS Security Policy Compliance," In: Proceedings of the 40th Hawaii International Conference on System Sciences, January 3e6, Los Alamitos, CA., USA, 2007.

Pechmann, C., Zhao, G., Goldberg, M., and Reibling, E. T. "What to Convey in Antismoking Advertisements of Adolescents: The Use of Protection Motivation

Theory to Identify Effective Message Themes," *Journal of Marketing* (67), 2003, pp. 1-18.

Plotnikoff, R. C., and Trinh, L. "Protection Motivation Theory." *Exercise and Sport Sciences Reviews* (38:2), 2010, pp. 91–98.

Ringle, C., Wende, S., and Will, A. SmartPLS (release 2.0 (beta)). (SmartPLS, Producer). (2005, 01 01). Retrieved 09 30, 2012, from SmartPLS : http://www.smartpls.de,

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

Rogers, R. W. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91), 1975, pp. 93-114.

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

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

Stair, R. M., and Reynolds G. *Principles of Information Systems*, Cengage Learning, 2012.

Sluski, L. and Partow-Navid, P. "Students Information Security Practices and Awareness," *Journal of Information Privacy and Security* (8: 4), 2012, pp. 3-26.

Stevenson, B. R., and Romney, G. W. "Teaching Security Best Practices by Architecting and Administering an IT Security Lab," In: Proceedings of SIGITE'04, October 28–30, 2004, Salt Lake City, Utah, USA, 2004.

Topi, H., J. S. Valacich, et al. "IS 2010: Curriculum Guidelines for Undergraduate Degree Programs in Information Systems," *Communications of the Association for Information Systems* (26:1), 2010.

Vance, A., Siponen, M., and Pahnila, S. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49), 2012, pp. 190-198.

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

Walden, J. "Integrating Web Application Security into the IT Curriculum," In: Proceedings of SIGITE'08, October 16–18, 2008, Cincinnati, Ohio, USA, 2008.

Wang, A. "Web-Based Interactive Courseware for Information Security," In: Proceedings of SIGITE'05, October 20–22, 2005, Newark, New Jersey, USA, 2005.

Woon IMY, Tan GW, and Low RT. "A Protection Motivation Theory Approach to Home Wireless Security," In: Avison D, Galletta D, DeGross JI, editors. Proceedings of the 26th International Conference on Information Systems, In Las Vegas, December 11-14, 2005, pp. 367-380.

AUTHOR BIOGRAPHY

Peter Meso is an Assistant Dean and Associate Professor of Information Technology in the School of Science and Technology at Georgia Gwinnett College (GGC). Dr. Meso's research papers appear in a number of journals, among them: Information Systems Research, Journal of the Association for Information Systems (JAIS), Information Systems Journal, European Journal of Information Systems, Communications of the ACM, Journal of Systems and Software to name a few. Prof. Meso also serves as co-editor in chief of the African Journal of Information Systems (AJIS).

Yi Ding is an Assistant Professor at Georgia Gwinnett College. He holds a Ph.D. in computer information systems (CIS) from the J. Mack Robinson College of Business at Georgia State University. His research interests include behavioral aspects of information system use in online service environment, computer forensics, computer security, software development methodology and the use of IT in education.

Shuting Xu is an Assistant Professor at Georgia Gwinnett College. Dr. Xu had her education at the University of Kentucky and Shanghai Jiaotong University. Her research is in the area of information systems security.