https://doi.org/10.48009/2_iis_2016_183-192

Issues in Information Systems
Volume 17, Issue II, pp. 183-192, 2016

CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS

Jackson Muhirwe, Central Washington University, jackson.muhirwe@cwu.edu
Nathan White, Central Washington University, Nathan.white@cwu.edu

ABSTRACT

College students have the highest adoption rates for Information Technology (IT), and tend to use IT for their personal things like shopping, socializing, and for education purposes. With more time spent in the cyberspace, there are also increased risk of cyberattacks. Students are at risk of identity theft and fraud through fraudulent emails, stolen passwords, and stolen social security numbers. Moreover, students as users on the college network may inadvertently commit cybercrimes. Lastly, students entering the workforce lacking cybersecurity awareness are at risk of contributing to the already well-known weakest link in organizational cybersecurity, the user. In this study, we investigated the relationship between cybersecurity awareness and practice for the next generation corporate technology users. Based on the analysis of the data collected in this study, cybersecurity awareness significantly impacts one's cybersecurity practice. While not effectively predicting one's awareness, cybersecurity training did show a significant relationship to cybersecurity awareness.

Keywords: Cybersecurity, Awareness, Practice, Cybercrime, College, Students

INTRODUCTION

Information Technology (IT) has penetrated every sphere of our lives. IT has provided us with enormous opportunities and conveniences that enrich every aspect of human lives. However, with all the opportunities also comes challenges. Taylor, Fritsch, & Liederbach, (2015) define cybercrimes as crimes committed with the aid of a computer. They further divide these crimes into four categories. First, crimes where the computers or networks are the target of a crime, such as denial of service attacks. Second, crimes where computers are instruments used to commit the crimes, such as fraud and cyber harassment. Third, crimes where computers are incidental to the crimes. These crimes would happen with or without use of computers, such as money laundering. The fourth and last category is crimes due to prevalence of computers. Examples of these cybercrimes include intellectual property violations, counterfeiting, and identity theft.

The FBI's Internet Crimes Complaint Center (IC3) reported in its 2014 annual report that they received 269,422 complaints with an adjusted dollar loss of $800,492,073 (FBI / IC3, 2015). On average, they received approximately 22,000 complaints each month. Cybercrimes have become a global issue with the sophistication of online criminal techniques and overlapping jurisdictional boundaries (IC3) (FBI / IC3, 2015).
The education sector has not been left behind by the opportunities and challenges of IT and has recently become a hot target for cyberattacks (Farooq, 2015). According to a recent report (May 2016) of the Identity Theft Resource Center (IDRC) data breaches in the Education sector increased by 53.8%. Reasons for the increase could be due to: 1) availability of vast computing power and 2) open access policies held by educational institutions. The breaches in higher education institutions could be from external or internal actors.

Cybersecurity is defined as the "ability to protect or defend the use of cyberspace from cyberattacks" (p. 22) (CNSS, 2010). Many cybersecurity professionals and researchers agree that users within an enterprise network are the weakest link to implementing effective and comprehensive cybersecurity (Jourdan, 2007). Based on an EDUCAUSE 2015, member institution survey, cybersecurity, which is also referred to as information security, continues to be an issue of "strategic importance" and ranked as the fourth most important issue.

Cybersecurity and the Next Generation Computer Users

Current college students are digital natives who comfortably use IT for their everyday lives and for almost every service they receive from their colleges. These services range from applying for admissions, enrolling for courses, attending classes, sitting for exams, to applying for graduation.

There are three dimensions that apply to the next generation of computer users: threats to student as computer users, students as network users, and students as future employees.

Threats to Students as Computer Users

Students as individuals using computers suffer from cyberattacks just like all other people. The risk of suffering from a cyberattack increases as the amount of time spent online increases. College students as millennials and digital natives spend a lot of time online, hence increasing their risk to suffer cyberattacks such as cyber stalking, spear phishing and social engineering. These are attacks could lead to financial loss, loss of identity, and even death.

Students as Network Users on a College Network

Students as users on campus enterprise systems have direct access to systems that enable them to do research and complete their school activities. As users on the network they can be channels for both intentional and unintentional attacks on organizational information assets.

Students as Future Employees upon Graduation

With all of the cybersecurity-related incidents reported in the media, the threat of a cyberattack is not unfounded. An organization's concern about cybersecurity is based on how dependent they are on technology. Leach (2004) suggested that insider threats were more pressing than external threats. This is largely as a result of poor user cybersecurity behaviors. Ernest and Young in their 2015 survey found that careless and unaware employees are the top vulnerability that corporations are concerned about (EY, 2015). Students lacking cybersecurity awareness entering the job market pose a threat to the hiring organization. Students as future employees being prepared to join the workforce need to be cybersecurity ready (Teer, Kruck, & Kruck, 2007). There's been an increasing demand for compliance to require written proof that cybersecurity awareness training has been conducted for specific high-risk groups of users. One such compliance requirement is HIPAA (Health Insurance Portability and Accountability Act) that requires employee awareness training to be conducted and documented. The earlier students are made aware of these compliance requirements; they are better at compliance. Targeted awareness programs and information security training expose students at an early stage to compliance requirements and what they should do when handling highly sensitive data.

In order to address the three dimensions of students related to cybersecurity, this study investigated the status of cybersecurity for college students at a medium-sized public university in the Pacific Northwest of the United States of America. This study also sought to find out whether training and awareness have a significant impact on students cybersecurity practices. The rest of the paper is organized as follows. The next section is a brief review of cybersecurity awareness. This is followed by the research methodology and finally we have the presentation and discussion of the results.

Cybersecurity Awareness

The terms cybersecurity and information security have been used in literature interchangeably. Popular media uses mostly cybersecurity and academic authors use mostly information security. The Committee on National Security Systems (CNSS) Glossary Working Group (CNSS, 2010) sought to resolve this debate by providing a glossary of terms in which cybersecurity is defined as the "ability to protect or defend the use of cyberspace from cyberattacks" (p. 22). CNSS (2010) defined information security as "the protection of information and information systems from

unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (p. 37). From the two definitions we can see that cybersecurity is a subset of information security. In this section we review information security awareness in reference to cybersecurity awareness.

An effective information program that addresses internal and external threats is implemented in three spheres: policies, people, and technology (Mattord & Whitman, 2014). Developing policies, guidelines, standards, and procedures simply marks the beginning of the process. Strong technical controls by themselves cannot provide all of the necessary security that organization's information assets require. These controls will be rendered useless if users are not trained and have cybersecurity made a part of their roles and responsibilities (Peltier, 2000). Information security researchers and professionals have identified insiders as the biggest threat to implementation of an effective information security program. In order address the insider threat, an organization needs to implement a Security Education, Training and Awareness (SETA) program (Mattord & Whitman, 2014). The main purpose of a comprehensive SETA program is to create awareness of the need to protect systems and information. Other purposes include developing skills and the deep knowledge to understand the what, why, and how of information security. The three elements of SETA differ by their definition and goals. Peltier (2000) defined education as the "the specialized, in-depth schooling required to support the tools or as a career development process" (p. 37). The goal of education is to provide insight and answer the "why" part of information security. Training is defined as the process through which one learns a skill or the required use of a tool. Training answers the "how" part of information security with the goal of imparting skills. Awareness is used to make users aware of their roles and responsibility in providing security to an organization's information and to their personal information they might be sharing in the cyberspace. The main goal of awareness is to provide information by answering the "what" of information security. Awareness programs are used stimulate, motivate, and remind the audience of what is expected of them.

There are two basic challenges to information security awareness that we would like to address. The first is: Is awareness the same as training and the second concerns the definition of awareness.
The key difference between awareness and training is derived from their unique goals. The goal of awareness is behavior change, while the goal of training is to impart skills as earlier defined.

Several researchers have attempted to come up with different definitions of information security awareness and what it takes to develop an effective information security awareness program. The definition that resonates with us and mostly agreed upon by many researchers and practitioners is the one given by the Information Security Forum (ISF, 2016). They define information security awareness as "the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities and act accordingly" (p. 1). Siponen (2001) defined information security awareness as "a state where users in an organization are aware, ideally committed to, of the security mission" (p. 31). Central to all the definitions of Information Security Awareness is the need to make users aware. How do we then make users aware? What awareness activities lead to behavior change that lead to safe computing practices in order to minimize compromises to information assets? Kruger and Kearney (2006) identified a set of factors which contribute to information security awareness. These factors are knowledge (related to what users know), attitude (what they think), and behavior (what they do). Several researchers have provided proposals on how to effectively conduct information security awareness. Traditionally, cybersecurity awareness has been done using low-tech methods such as creating and distributing posters or flyers. These efforts can be compared to "throwing efforts into a bottomless pit". There is no easy way to develop meaningful metrics on how effective these types of security awareness activities are and whether they actually influence behavioral change (EDUCAUSE, 2015). An awareness message is generally more effective if it is targeted to a specific audience. In this same study, respondents to Educause survey provided the following information for the awareness activities they carry out:

- Only training – 57%
- Website Education materials 54%
- Email 51%
- Cybersecurity Awareness Month 32%
- Instructor–led training 26%
- Customized workshops 15%

- Targeted risk prevention training 14%
- Social networking tools 12%
- Others 9%

Research Questions

For the purpose of this study, the goals of the study were framed in terms of the following three research questions:

1. Does the number of cybersecurity training classes a student has attended have a significant impact on their cybersecurity awareness?
2. Does the number of cybersecurity events a student has attended have a significant impact on their cybersecurity awareness?
3. Does an individual's cybersecurity awareness level impact their cybersecurity practice?

RESEARCH METHODOLOGY

Introduction and Study Hypotheses

Our research centered upon the following general research question: is there a significant relationship between cybersecurity awareness and safe computing practice? Following the specific research questions developed after the literature review, the following hypotheses were developed to be tested as follows:

H1 – The number of cybersecurity training classes a person has attended will not significantly impact their cybersecurity awareness.
H2 – The number of cybersecurity events a person has attended will not significantly impact their cybersecurity awareness.
H3 – An individual's cybersecurity awareness level will not impact their cybersecurity practice.

The hypotheses are summarized in the research model adopted for this study and presented here as Figure1.

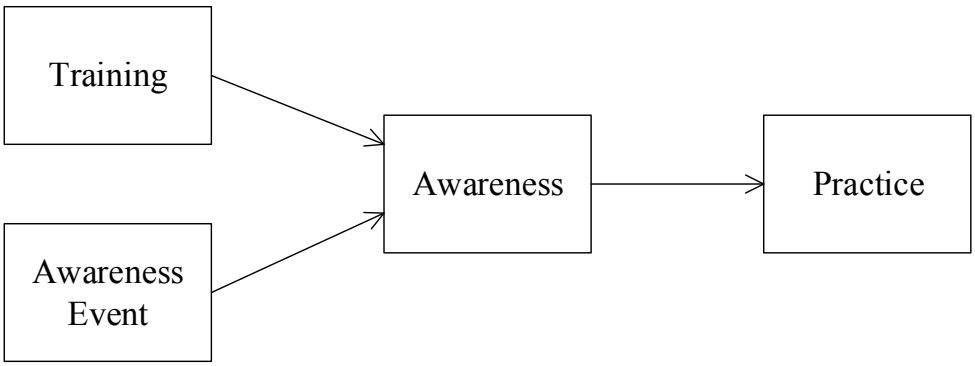

Figure 1. Research Model

Instrument Development

In order to answer the research questions and test the hypotheses, we developed a comprehensive survey tool. The survey awareness questions were based on the NIST 800-50 publication, which recommends 27 topics in order to have an effective cybersecurity awareness program (NIST, 2016). Other survey questions were added from a

literature review conducted on recent studies on cybersecurity awareness amongst students in higher education. The survey instrument was developed in Qualtrics as a modification of the information security awareness instrument developed by (Nyabando, 2008).

The survey instrument was comprised of four parts. The first part consisted of cybersecurity awareness (CSA) questions. A question was added to record the perceived CSA and knowledge of the respondents; a five point Likert Scale was used for this purpose. The second part was about cybersecurity awareness and training events. Respondents were asked to report about where they learned about cybersecurity. The goal of these questions was to help us know which cybersecurity awareness and training events are effective in reaching many students. The third part consisted of questions relating to cybersecurity practices (CSP) and behaviors. These questions were formulated to discover the cybersecurity practices of the respondents. A five scale Likert scale was used. In these questions, our goal was to find safe and unsafe computing practices. The last part was demographic questions. Demographic questions were used as control variables and to investigate if awareness was different for people of different genders. Additional demographic questions that were added as control variables include questions on age, academic status, number of years using a computer, and major subject of study. Table 1 lists the questions that were used in our survey instrument.

Table 1. Survey Questions on Cybersecurity Awareness and Practice

Category	Main Question	Sub-questions	Scale
CSA	With respect to information technology and cybersecurity, I am aware….	• of the requirements for computer use policies at my college • expectations of the computer use policies at my college • of the impact that a virus and other malicious software can have on my computer system • that virus protection software can identify and remove viruses • that virus protection software requires frequent updates • that I should keep my passwords secure • of the impact of responding to phishing emails (e.g. unsolicited emails asking for your bank information) • that encryption can prevent unauthorized access to confidential information of the vulnerabilities associated with sharing devices such as files and drives	5-point Likert Scale
CSA Events and Training	• I have attended a cyber security awareness event • I have attended a cyber security training class	None	Various locations given
CSP	To what extent do you do the following?	• I log off or lock my computer before I step away from my computer • I log off when I finish using a computer system • I back-up my files on reliable media • I back-up my files using cloud services such as OneDrive and google drive • I have antivirus software on my home computers • I keep the antivirus software on my computer updated • I allow programs to save my usernames and passwords for faster access in the future • I download and install programs from the internet as I deem necessary on my computer • I check whether a website is secure or not before making a financial transaction over the internet • I seek out information about cyber security	5-point Likert scale

		• I open emails regardless of not knowing the sender's identity • I open email attachments regardless of knowing the sender's identity • When choosing a password, I use a combination of letters, numbers and special characters • I protect confidential files with passwords • I share my password with other people • I write down my password • I change my password(s)	

Data Collection

An online survey was created and distributed to the subjects using a web-based survey service provider. Qualtrics was selected because it is highly secure, provides tools for preliminary review of results, and supports exporting of responses to many external tools as SPSS. Qualtrics provides support for many different forms of questions ranging from multiple-choice to descriptive text.

Distribution of the survey to the students was done via email. The email invited all students to voluntarily participate in the research, clearly stating that their responses will remain strictly anonymous. Therefore, no name or other identifying information was collected from any respondent and no metadata was collected in any form that could be used to identify the respondents. The invitation email further provided details about the purpose of the study. The study required the subjects to be current registered students and 18 years of age or older. The first part of the survey instrument was an introduction which provided the purpose of the study and asked the respondents to provide their consent.

The survey instrument used for this study was distributed to the students of a medium-sized, regional university in the Pacific Northwest of the United States. Two hundred forty-nine individuals started the survey. Two individuals did not provide their consent. Another 33 respondents abandoned the survey without submitting their responses. The remaining 214 respondents completed the survey in its entirety.

This research gathered five types of demographic information: gender, age, academic status, number of years of computer use, and technical nature of the individual's major. Of the respondents, 49% were males and 51% were females. This data is representative of the university population, as the actual ratio of males to females for the whole university is 49:51. Table 2 summarizes this information.

Table 2. Demographic Information

Distribution by Gender		
Item	Frequency	Percentage (%)
Male	105	49%
Female	109	51%
Distribution of Age		
Item	Frequency	Percentage (%)
18-20	53	25%
21-25	65	30%
26-30	31	14%
31-40	31	14%
41-50	17	8%
Above 50	17	8%
Distribution by Academic Status		
Freshman	17	8%
Sophomore	21	10%
Junior	85	40%

Senior	82	38%
Graduate	9	4%
Distribution by Number of Years Using a Computer		
< 1 Year	3	1%
1 – 5 Years	5	2%
6 – 10 Years	41	19%
More than 10 Years	165	77%
Distribution by Major		
Technical	98	46%
Non-technical	116	54%

RESULTS

Pre-analysis Data Screening

Prior to assessing the structural model, the collected data was assessed for any irregularities following the guidance of Hair et al. (2014). The initial step in this process was to check for missing data. All 214 respondents who completed the survey did so completely and there was no missing data. The next step was to assess the data for an suspicious patterns, such as response sets (Levy, 2008). No suspicious response patterns were found in the data. The final pre-analysis screen step was to check for outliers, which was done with the Mahalanobis Distance statistical test. No outliers were found.

Indicator Assessment

Using the steps outlined by Hair et al. (2014), the reflective constructs' indicators in our model were assessed using SmartPLS 2.0 and SPSS. Checking the internal reliability of the constructs was the first step. As recommended by Hair et al. (2014), composite reliability (ρ_c) and Cronbach's Alpha were used. Indicators that lowered either of those two measures were removed from the model. Once these indicators were removed, the Cronbach's Alpha of Awareness was 0.90 and Practice was 0.77. Similarly, the ρ_c of both indicators were found to be satisfactory, with Awareness having a ρ_c of 0.92 and Practice having a ρ_c of 0.85. Determining convergent validity was the next step recommended by Hair et al. (2014). The Practice indicators that lowered the average variance extracted (AVE) below 0.50 were removed. After those indicators were removed, all but four had outer loadings above 0.70. Two Awareness indicators and two Practice indicators had an outer loading between 0.40 and 0.70. As recommended by Hair et al. (2014), these indicators were left in the model as the AVE for each construct was above 0.50. The final step in assessing the reflective constructs was to determine if the constructs displayed good discriminant validity (Hair et al., 2014). Cross loading and Fornell-Larcker criterion were used and both tests indicated that all indicators loaded on the appropriate constructs. Table 3 summarizes the assessment of the reflective constructs.

Table 3. Reflective Constructs

Variable	Indicator	Outer Loading	Indicator Reliability	Composite Reliability	Cronbach's Alpha	AVE	Discriminant Validity
CSA	CSA1_10	0.8457	0.7152	0.9215	0.9033	0.5963	Yes
	CSA1_3	0.7938	0.6301				
	CSA1_4	0.7853	0.6167				
	CSA1_5	0.7781	0.6054				
	CSA1_6	0.6520	0.4251				
	CSA1_7	0.6901	0.4762				
	CSA1_8	0.7868	0.6191				

	CSA1_9	0.8263	0.6828				
CSP	CSP1_10	0.7299	0.5328	0.8456	0.7699	0.5257	Yes
	CSP1_3	0.6276	0.3939				
	CSP1_5	0.7655	0.5860				
	CSP1_6	0.8402	0.7059				
	CSP1_9	0.6404	0.4101				

Structural Model Assessment

In assessing the structural model, collinearity, path coefficients, and the coefficient of determination (R^2) were used (Hair et al., 2014). The variable inflation factor for both predictor variables was below 5.0, indicating the lack of collinearity. The path coefficients were then computed and are shown in Figure 2. The path coefficients from Training to Awareness and the path from Awareness to Practice showed significance to $p < 0.001$. The path coefficient from Event to Awareness was not significant. The R^2 values for the endogenous variables are also shown on Figure 2. Practice showed good predictive accuracy, while Awareness did not.

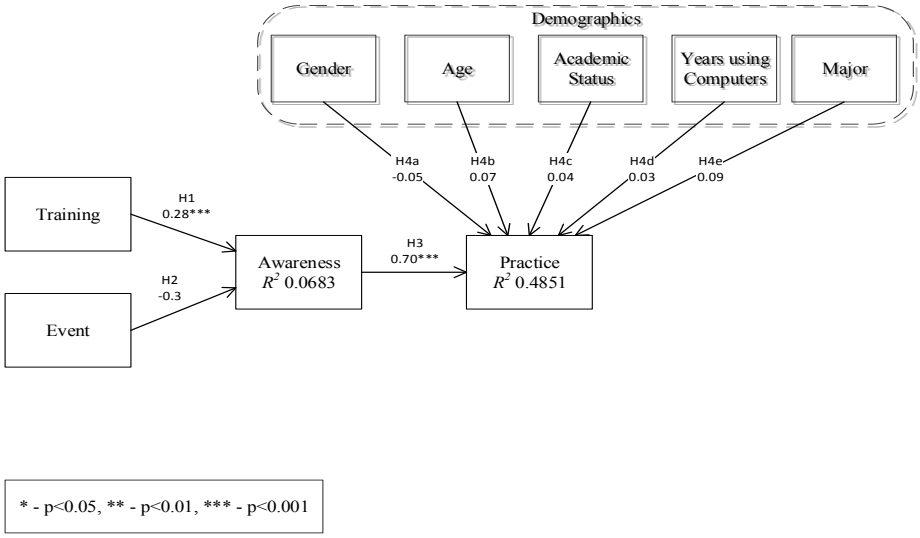

Figure 2. Path Coefficients

DISCUSSION

Summary of Results

The tests of each of the hypothesis are summarized in Table 4. Based on the analysis of the data collected in this study, cybersecurity awareness significantly impacts one's cybersecurity practice. While not effectively predicting one's awareness, cybersecurity training did show a significant relationship to cybersecurity awareness. However, cybersecurity events did not significantly impact one's cybersecurity awareness. Similarly, none of the control variables collected in this study showed any significant impact on cybersecurity practice. These results will be shared with our university's IT security department in an effort to improve the cybersecurity awareness and practice of our students.

These results indicated that cybersecurity training classes have a greater potential to affect the cybersecurity awareness and practice of college students than cybersecurity awareness events. Regardless of age, gender, major, academic status, or years of computer experience, cybersecurity training is better suited to this population of students that will soon be employees. In order to protect their networks, universities and businesses should evaluate how they invest in raising the cybersecurity awareness of this population to ensure they make the most effective use of their time and money.

Table 4. Summary of Hypotheses Results

Hypotheses		Path	Results
H1:	The number of cybersecurity training classes a person has attended will not significantly impact their cybersecurity awareness.	Training -> Awareness	Partially Supported
H2:	The number of cybersecurity events a person has attended will not significantly impact their cybersecurity awareness.	Event -> Awareness	Supported
H3:	An individual's cybersecurity awareness level will not impact their cybersecurity practice.	Awareness -> Practice	Not Supported

CONCLUSIONS

Results from this study do indicate that cybersecurity awareness significantly impacts one's cybersecurity practice. It is therefore important that colleges organize regular cybersecurity awareness activities that are targeted to different students at different levels of study. Cybersecurity awareness events should be included in the orientation program for freshmen. Many colleges host the National Cybersecurity Awareness Month (NCSAM) in October and then wait for a whole year to organize similar events. Whereas participating in NCSAM is good, it is not sufficient to cause the much needed behavior change. Awareness events need to be scheduled regularly and spread throughout the year using formal and information events. Although, cybersecurity training only partially impacted awareness, it is recommended that a combination of awareness events and training be organized for all students before they graduate. This will ensure that colleges do not graduate students with unsafe computing practices. In consideration of this, our department has already added an introduction to cybersecurity as part of the core curriculum in all of its undergraduate programs.

Future research could include a longitudinal study, which would test awareness at the beginning of school year, shortly after the NCSAM, and then later in the school year. Additionally, a qualitative study could also be performed that would interview students who have attended cybersecurity events. Determine why they attended and what, if any, impact the events had upon their awareness and practice. Further studies could also track these current students after they graduate and see what, if any, changes to their cybersecurity awareness and practice take place and what caused those changes to take place.

REFERENCES

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organization and End User Computing, 16*(3), 22-40.

CNSS. (2010). *National Information Assurance (IA) Glossary CNSS Instruction No. 4009.* Washington DC: Committee on National Security Systems (CNSS) Glossary Working Group.

Educause. (2015). *Top 5 strategic information security issues for 2015.* Louisville: Educause.

EY. (2015). *Creating trust in the digital world: EY's Global Information Security survey 2015.* London: Ernest and Yound.

Farooq, A. I. (2015). Information security awareness in education institution: An analysis of student's individual factors. *Trustcom/BigDataSE/ISPA, 2015 IEEE.* Helsinki: IEEE.

FBI / IC3. (2015). *2014 Annual Crime Report.*

Hair, J. F. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM).* Thousand Oaks, CA: Sage.

ISF. (2016). *The standard of good practice for information security Information security forum.* London: Information Security Forum.

Jourdan, Z. (2007). Computer security knowledge and training: Where do students learn about computer security? *SEDSI*, (pp. 399 – 499). Savannah, GA.

Kim, E. B. (2013). Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective, 22*(4), 171-179.

Kruger, H. A. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296.

Leach, J. (2003). Improving user security behavior. *Computers and Security, 22*(8), 685-692.

Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers and Education, 51*(4), 1664–1675.

Mattord, M. E., & Whitman, H. J. (2014). *Principles of Information Security.* Boston: Cengage Learning.

McElroy, L., & Weakland, E. (2013). Measuring the effectiveness of security awareness programs. *Educause Research Bulletin*.

NIST. (2003). *Special Publication 800-50: Building an information technology security awareness and training program.* Washington DC.

Nyabando, C. J. (2008). *An analysis of perceived faculty and staff computing behaviors that protect or expose them or others to information security attacks.* Electronic Theses and Dissertations. Paper 1972. http://dc.etsu.edu/etd/1972.

Peltier, T. (2000). How to build a comprehensive security awareness program. *Computer Security Journal, 16*(2), 23-32.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security, 8*(1), 31-41.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism.* Upper Saddle River, NJ: Prentice Hall Press.

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empiracal study of students' computer security practices/perceptions. *Journal of Computer Information Systems, 47*(3), 105-110.