Cybersecurity Training and the End-User: Pathways to Compliance

Dinesh Reddy
dinesh.reddy@utsa.edu

Glenn Dietrich
glenn.dietrich@utsa.edu

The University of Texas at San Antonio
1, UTSA Circle, San Antonio TX 78249

Abstract - In order to effectively combat cybersercurity threats at home and in organizations, it is imperative to achieve higher end-user cybersecurity compliance. Cybersecurity training is generally accepted as a means to increase compliance behavior. Training can influence compliance by one or more of three causal pathways: by increasing cybersecurity awareness, by increasing cybersecurity proficiency (i.e., improve cybersecurity skills) and by raising cybersecurity self-efficacy. The effects of awareness and self-efficacy on compliance have been empirically examined and reported in literature, but the effect of cybersecurity skills has not received much attention. In an effort to understand the pathways through which training affects compliance, we develop a theoretical model and offer propositions. The model helps us understand how cybersecurity training should be designed and executed to optimally influence each of the three pathways to compliance and finally to have an optimal impact on compliance. Empirical validation will be performed at a later stage. Results of the study are expected to help design training programs to enhance end-user cybersecurity skills and consequently cybersecurity compliance.

Categories and Subject Descriptors

K.5.2 [Legal Aspects of Computing]: *Governmental Issues – Regulation*

General Terms

Training, Security

Keywords

Cybersecurity training, cybersecurity skill, cybersecurity awareness, self-efficacy in information security, cybersecurity compliance

1 INTRODUCTION

> *"…the human remains the weakest link in the information security chain." (Eric Savitz, 2011)*

The idea that the end-user is the weakest link in the security chain has been repeated by many scholars and practitioners. There are some who object to this perspective arguing that it is used as a cover for the failure to design effective and usable safeguards. Regardless of whether one believes that users are the weakest link, it must be accepted that end-user behavior can often lead to lapses in security. Such lapses are often attributed to a lack of awareness of security issues. For instance, a SANS institute report suggests that "A Security Awareness program is probably the most important weapon in the Information Security professional's arsenal." (SANS Institute, 2001). Awareness programs provide guidelines such as use strong passwords, use a different password for each account, do not post the password on the computer screen and so on, but fail to educate the user on other issues, such as interpreting warning messages and responding appropriately. Savitz (2011) remarks, "We're all familiar with the obscure "certificate warnings" that our Web browsers occasionally grace us with – these warnings are completely indecipherable, un-actionable, and thus routinely ignored." This suggests that cybersecurity training programs may need to go beyond simple awareness education. Our research is based on the premise that training needs to include sufficient knowledge to understand messages and know what responses are appropriate, and, the development of skills to execute the steps to protect the information residing in the computer in the event of a threat.

End-user training is recognized as an important component of the steps necessary to improve cybersecurity compliance, and consequently cybersecurity posture. Antecedents of cybersecurity compliance in both the home and organizational context have been studied. Among the individual factors that have been examined are cybersecurity awareness, self-efficacy in information security and, to a lesser extent, cybersecurity skills. Each of these variables is potentially a mediator between cybersecurity training and compliance. Research has not examined either the mediating role of these three factors, nor has it examined the relative effectiveness of these measures in achieving compliance. Hence the research questions that will be pursued in our research are:

1. What factors mediate the relationship between cybersecurity training and compliance?
2. What is the relative effectiveness of each factor on improving compliance?
3. How does the nature of training affect each of the mediating variables?

In the current article, we develop the research model and provide supporting arguments for the relationships proposed.

The rest of the article is organized in the following manner: First, we present literature review on key concepts related to cybersecurity compliance, training, awareness, self-efficacy in information security and cybersecurity skills followed by the propositions and the research model. Next, we discuss the proposed methodology to test the research model. Finally, we conclude with practical implications and future research.

2 LITERATURE REVIEW

2.1 Cybersecurity Compliance (CC)

End user CC is a specific case of cybersecurity behavior in which computer users show conformity with the safe and secure rules and policies, and comply with a recommended course of action (Johnston and Warkentin 2010, Herath and Rao 2009). Table-1 provides a summary of a sample of studies in which CC is the dependent variable. There are several points that can be seen in the table. First, cybersecurity compliance has been studied both in organizational and home context. In organizational context, the studies have been conducted at both organizational and individual level of analysis. In the home context, studies have been at the individual level of analysis. The model that is being developed in our research is for the individual level of analysis, and should be applicable in both the home and organizational context.

CC is difficult to achieve for many reasons. For example, Herath and Rao (2009) state that computer users are most likely to discard the secure rules and policies as mere steps and guidelines, rather than considering the secure policies as standards that help achieve cybersecurity. CC is critical since the negligence and non-compliance by individuals and employees of an organization will lead to significant financial losses caused by data breaches (PrivacyRights website 2016).

Several predictors of CC have been studied in prior research, such as fear deterrence, fear appeals, user awareness and so on. The effectiveness of the antecedents is likely to vary based on the motivation of the users to comply or conform to security policies. Users can be classified into unwilling conformers, reluctant conformers and the willing conformers. Unwilling conformers need effective deterrence measures to motivate them. The reluctant conformers may be motivated by fear appeals, social influence, threat perception and so on. Willing conformers are motivated to comply with cybersecurity guidelines and policies, but may be hampered by their lack of awareness of potential threats, their lack of understanding of security related issues, and their lack of skills to take the necessary steps to protect information assets. In the current study, our focus is on enabling the willing conformers to achieve a stronger security posture through appropriate training. In Table 1, it can be seen that awareness has received much attention, self-efficacy has received some attention and cybersecurity skills have only recently received some attention, suggesting the need for more research on these factors.

Compliance as DV Papers	**Level**	**Context**	**Predictors of Compliance**
Rhee et al. 2009	Individual	Home	Self-efficacy in information security, computer/internet experience, security breach incidents, general controllability.
Johnston & Warkentin 2010.	Individual	Org	Fear appeals, self-efficacy, response efficacy, threat severity, social influence.
Bulgurcu et al. 2010	Individual	Org	Information security awareness.
D'Arcy et al. 2009	Org	Org	User Awareness of security countermeasures, sanction perceptions.
Herath & Rao 2009	Individual	Org	Severity of penalty, certainty of detection, Normative beliefs, peer behavior, perceived effectiveness.

Compliance as DV Papers	**Level**	**Context**	**Predictors of Compliance**
Lee et al. 2004	Org	Org	General deterrence factors such as security policies and security awareness.
Blanke 2008	Individual	Org	Computer security policy awareness.

Table-1 Summary of Past Literature on Cybersecurity Compliance

2.2 Cybersecurity Training (CT)

In business environments, the need for the implementation of security countermeasures such as CT has been emphasized and recommended in order to reduce IS computer abuse (Straub and Welke 1998). Security policies form the basis for security education training and awareness (SETA). CT sessions in general are aimed at informing the users about unacceptable system use and penalties for noncompliance (Straub 1990). CT is defined as those activities that impart specific cyber skills such as safe internet browsing, encryption, decryption and system manipulation (Torkzadeh and Van Dyke 2002), in order to make security decisions (Furman et al. 2011). The ultimate goal of CT is to impart knowledge and skills such as vulnerability analysis and mitigation, intrusion detection and incident response, in order to be less susceptible to social engineering.

Some of the common training techniques include formal training, passive computer-based and web-based training, and interactive computer-based training (Cone et al. 2007). The different aspects of training effectiveness are evaluated using measures such as reaction, learning, cognitive, and behavioral criteria. (Frayne and Latham 1987). The reaction criteria measure the extent to which trainees liked the training content, and the perceived relevance of the training to trainee's needs. The learning criteria assess the knowledge and skills gained during the training. Prior computer knowledge, computer experience, computer playfulness, and performance during training are all shown to affect post-training effectiveness (Potosky 2002, Puhakeinen and Siponen 2010). However, two studies were identified that examined the effect of CT on CC and the results of these studies are mixed as shown in Table 2.

Study	**Training Increase Compliance**	**Key Finding**	**Metho dology**	**Sample**
Lee et al. 2004	No	Self-defense intention (SDI) arising out of training increases computer abuse.	Survey	500 MBA students and 500 middle managers in six companies in Korea.
Straub 1990	Yes	Training sessions reduce abuse.	Survey	IS directors. Middle IS managers, IS security officers, controllers, auditors, programmers, analysts, etc.

Table-2 Summary of Past Literature on Cybersecurity Training

2.3 Cybersecurity Awareness (CA)

CA is defined as the state of being cognizant of performing secure tasks on a computer (Bulgurcu et al. 2010). Studies have focused on different aspects of awareness. For instance, some have examined awareness of computer usage policies (e.g., Cronan et al. 2006), others have examined security countermeasures (e.g., D'Arcy et al. 2009) and so on. The multiple aspects collectively include comprehensive information about general guidelines of information security, basic education on security risks and consequences of cybersecurity threats, and tracking internet usage for abnormal activities (Choi et al. 2013). All awareness aspects listed in table-3 can be categorized into three dimensions. One such dimension of awareness is related to security policies where a computer user is aware that there are detailed set of guidelines to guide the user in understanding what actions on computers are safe and secure (D'Arcy et al. 2009). Another dimension of awareness refers to trainings where a computer user is aware that there are training programs available to educate users on acceptable safe and secure usage of computers, and the risks involved in misusing the computers. Yet another dimension of awareness refers to tracking internet usage by service providers where a computer user is aware that their computer activities are under surveillance and that any misuse of computer will be detected as unusual behavior (Choi et al. 2013). Table-3 lists past studies on the effect of CA on CC, and the results are mixed at best.

Compliance as DV Papers	**Cybersecurity Awareness Aspect**	**Awareness Increases Compliance?**
Bulgurcu et al. 2010	Information security awareness	Yes
D'Arcy et al. 2009	User awareness of security countermeasures	No

Compliance as DV Papers	**Cybersecurity Awareness Aspect**	**Awareness Increases Compliance?**
Aytes and Connolly 2004	Awareness of safe practice, awareness of negative consequences	No
Dinev and Hu 2007	Technology Awareness	Yes
Lee et al. 2004	Security awareness	No
Cronan et al. 2006	Awareness of computer usage policies	No
Foltz et al. 2005	Awareness of computer usage policies	No
Choi et al. 2013	Cybersecurity countermeasures awareness	No

Table-3 Summary of Past Literature on Cybersecurity Awareness

2.4 Self-Efficacy in Information Security (SEIS)

The perception of efficacy as per Witte (1994) includes the cognitions of the efficacy of recommended response and the efficacy of the individual in performing that response. The latter is known as self-efficacy and is defined as the degree to which individuals believe in their abilities to organize and execute a particular course of action (Bandura 1986; Vishwanath et al. 2011), and enact the recommended response (Johnston and Warkentin 2010). Self-efficacy is people's belief in their abilities to mobilize the motivation, cognitive resources, and courses of action needed to exercise control over given events and perform the tasks successfully (Ozer and Bandura, 1990). Ng et al. (2009) defines self-efficacy in terms of an individual's self-confidence in his/her ability to perform a behavior. Social cognitive theory has self-efficacy as an important construct, which is a form of self-evaluation that is nearest determinant of individual behavior, and also influences the amount of initiation, effort, self-regulation and persistence of coping efforts to overcome obstacles (Bandura 1986). Bandura (1977) identified four important factors that affect self-efficacy beliefs as listed in table-4.

Factor	**Description**
Enactive experience	Self-efficacy is increased by performing a behavior successfully.
Vicarious experience	Self-efficacy is increased when other people holding similar interests of that of an individual are performing a behavior successfully.
Verbal persuasion	Self-efficacy is influenced by encouragement and discouragement pertaining to an individual's performance.
psychological and affective states	Self-efficacy is influenced by an individual's own anxiety and stress

Table-4 Self-Efficacy Model (Bandura 1977)

Computer self-efficacy (CSE) which is derived from self-efficacy is defined as an individual's judgment of his/her capability to use a computer in various situations (Compeau and Higgins 1995; Vishwanath et al. 2011). Marakas et al. (1998) explains the concept of CSE at 'general level' that applies to multiple computer domains and 'task specific level' which applies to specific computer-related tasks within the domain of general computing. Adapting the general definition of CSE to the more specific information security context, SEIS is defined as a belief in an individual's capability to protect information systems from unauthorized disclosure, loss, modification, destruction and lack of availability (Rhee et al. 2009). SEIS refers to an individual's self-confidence in his/her abilities in practicing computer security that is likely to increase computer security behavior (Ng et al. 2009). SEIS is also defined as the user's confidence in taking the safeguarding measure and is an important determinant of threat avoidance motivation (Liang and Xue 2009; Liang and Xue 2010).

SEIS is examined as a direct determinant of behavioral intent of end user CC (Johnston and Warkentin 2010). Self-efficacy is one of the most popular variables found by the systematic review of research on variables that affect compliance with information security policies of organizations (Sommestad et al. 2014). It was also found that while each of the 40 variables was only investigated in a single study, self-efficacy was investigated in 7 studies. Two studies also proved consistent results in linking self-efficacy with actual compliance (Sommestad et al. 2014). Prior studies have examined very few antecedents to SEIS. Johnston and Warkentin (2010) have shown the impact of perceptions of threat severity to be negative on SEIS. Results from the same study also show the impact of threat susceptibility to be positive on SEIS. Rhee et al. (2009) have examined the effect of prior experience in computers and internet, security breach incidents and general controllability of information security threats on SEIS.

2.5 Cybersecurity Skills (CS)

Skill is defined as "a combination of ability, knowledge and experience that enables a person to do something well" (Boyatzis and Colb 1991: pg280). On similar lines, Torkzadeh and Lee (2003) define skill as the ability to understand and apply the intellectual abilities to accomplish the most appropriate action for the best result. Skills influence an individual's experience, behavior and attitude (Choi et al. 2013) and increase efficiency and positive behavior (Carruth et al. 2010). End user computing skill is referred to as an ability to utilize computer software and hardware in order to design, develop, modify and maintain applications for task-related activities. One specific form of computing skill is defined by Torkzadeh and Lee (2003) as IT skill, which is the knowledge and ability to use computer software, hardware and procedures for specific computer application development. On similar lines, we derive yet another specific form of computing skill to be CS, which encompass the capability to effectively utilize computer security programs such as antivirus programs. Hence, computing skills form the foundation of CS, since an appropriate level of computing skills is needed to effectively learn and utilize the cybersecurity knowledge.

Extending the definition of end user computing skill given by Torkzadeh and Lee (2003) to cybersecurity domain, CS is defined as the capability to practically apply intellectual abilities such as cybersecurity tools (e.g., anti-virus, anti-spyware) in order to protect the sensitive data stored in a computer (Rezgui and Marks 2008). CS can represent either technical abilities or non-technical abilities or a combination of both. Technical abilities involve utilizing technical knowledge and experience on software and hardware needed for performing secure activities on computers (Lerouge et al. 2005) and to effectively utilize cybersecurity innovations and functions. Applying this concept, Lerouge et al. (2005) studied the appropriateness of skill set of a systems analyst in order to effectively utilize and explore technology. They found the relevance between each skill dimensions and the role played in utilizing that skill. Non-technical abilities involve motivational factors from within a user to seek out the most appropriate knowledge that is needed to safeguard the computer, and repeatedly performs the secure actions in order to gain cybersecurity experience without being aware of the technical details (Rank et al. 2004, Dworkin et al. 2003). In the current article, we limit the term CS to the technical skills only.

3 RESEARCH MODEL[1] AND PROPOSITIONS

Training has been generally shown to have an improvement in the awareness levels. Training is the universal panacea recommended to raise security awareness (e.g., Brodie 2008). Furthermore, there is empirical evidence to support that training improves awareness levels (Eminagaoglu et al. 2009). Hence,

Proposition 1a: Cybersecurity training positively influences cybersecurity awareness.

The need for CA to increase CC has been argued in both the academic venue (Siponen 2000) and the commercial venue (NICCS 2015). But empirical evidence of the effect of CA on CC has been mixed as discussed earlier in table-3. The causal link between CA and CC in our model is being argued on a logical basis rather than on the basis of empirical evidence. Users who are unaware of the existence of cybersecurity problems are unlikely to seek solutions for them. Further, users who lack an awareness of solutions will fail to take necessary steps to ensure cybersecurity.

Proposition 1b: Cybersecurity awareness will positively influence cybersecurity compliance.

Computer training has been shown to affect CSE by determining multiple levels of CSE (Cassidy and Eachus 2002). Studies have also shown that training has a positive effect on self-efficacy and that post training, self-efficacy positively affects performance (Gist et al. 1989, Torkzadeh et al. 1999, Marakas et al. 1998). On the basis of this, it can be argued that CT will influence SEIS.

[1] The proposed model subsumes an earlier model (relating CA, CC and CS) that we have published at another venue.

Proposition 2a: Cybersecurity training will positively influence self-efficacy in information security.

Individuals with higher SEIS also have stronger intentions to strengthen cybersecurity. Johnston and Warkentin (2010) have shown that SEIS has a positive effect on an individual's intentions to adopt recommended computer security actions. Rhee et al. (2009) have shown that individuals with higher SEIS tend to use more security protection software and demonstrate more security conscious behavior. Individuals with higher SEIS also have stronger intentions to put more effort to strengthen cybersecurity (Rhee et al. 2009).

Proposition 2b: Self-efficacy in information security will positively influence cybersecurity compliance.

Computer training experiences have been shown to enhance the skill set of a computer user both at individual and organizational level (Marakas et al. 1998).

Proposition 3a: Cybersecurity training will positively influence cybersecurity skills.

The skills theory posits that in any field, a specific skill results in specific cognitive development that directly affects behavior. If the cognitive development happens in a sequence, then a particular skill is controlled on each developmental sequence, and each skill gradually goes up from one level to another in the developmental sequence (Fischer 1980). This implies that as the developmental levels go higher the resulting skill structure, will have an incremental effect on the behavior. The behavior is not uniform across all developmental levels due to difference in the skill structure. Udo et al., (2010) apply this concept to learning process in web services field, where the learning process captures unique inclinations of customers and individual differences in skill levels. Carlton and Levy (2015) take a similar approach and state that a skill is acquired over a period of time in three stages from initial acquisition of knowledge to converting that into procedural knowledge which is more organized, and progressing towards an experienced level. Extending this to the area of cybersecurity, it can be argued that CT will increase CS. In the case of motivated conforming users, if users possess high levels of the necessary CS to comply, then CC will be correspondingly high. If users do not possess adequate skills, then compliance will be correspondingly low. On the basis of this, it can be stated that CC will be positively correlated to CS. Combining the relationships between CS and CC, it can be said that:

> *Proposition 3b: Cybersecurity skills will positively influence cybersecurity compliance.*

Studies show that awareness in general improves self-efficacy. For instance, awareness has been shown to significantly increase internet and computer self-efficacy (Torkzadeh et al. 2006). Rezgui and Marks (2008) mention that regular update on security policies and relevant awareness initiatives will prevent users from underestimating the dangers caused by their actions. Such cognizance will enhance the confidence of users in relation to security-related matters. This leads us to the next proposition.

> *Proposition 4: Cybersecurity awareness will positively influence self-efficacy in information security.*

The ability to learn a computer skill and being proficient in using that skill is closely related to computer self-efficacy (Compeau and Higgins 1995; McCoy 2010). Skills closely relate to self-efficacy and individual reactions to technology usage and adoption (Compeau et al. 1999). Studies also found that both computer proficiency and computer self-efficacy are results of user's skill level development and transformation (Fischer 1980; McCoy 2010). Choi et al. (2013) has shown that an individual's ability to detect and remove suspicious malware software hidden in the computer is significantly correlated to the same individual's perceptions about his/her ability to detect and remove suspicious malware software hidden in the computer. This leads us to the following propositions that relate CS and SEIS.

Proposition 5: Cybersecurity skills positively influence self-efficacy in information security.

The effect of CA on CC may be mixed. In particular, a user who is aware of a solution but is not proficient to implement the solution may fail to comply with the necessary cybersecurity steps. In contrast, a user who is aware of the solution and has the necessary skills to implement the solution will succeed in complying. Thus, it can be seen that CS has a moderating effect on the relationship between CA and CC.

Proposition 6a: Cybersecurity skills will moderate the effect of cybersecurity awareness on cybersecurity compliance.

Similarly, a user who has high self-efficacy but low level of skills may not be able to comply with security requirements. In contrast, a user who has high self-efficacy and high level of skills will be able to comply. In effect, security will moderate the effect of SEIS on CC.

Proposition 6b: Cybersecurity will moderate the effect of self-efficacy in information security on compliance

Figure-1 shows the research model based on the propositions which will be tested empirically.

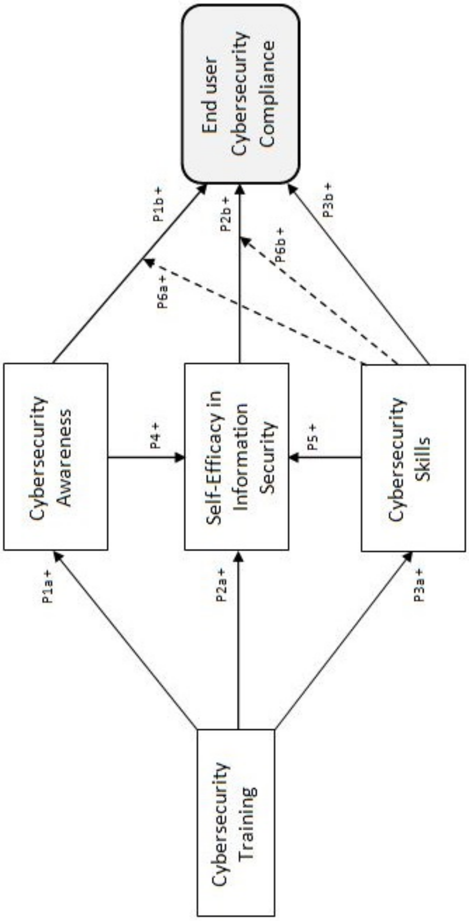

Figure-1 Research model

4 PROPOSITION METHODOLOGY

Survey methodology is planned to empirically validate our proposed research model. Survey items will be adopted from past research and suitable modifications will be made as applicable to this study. Initial survey items will be reviewed by experts in the field. Reliabilities and content validities of all survey items will be ensured before the items are used in actual data collection. Target population for this study will be university undergraduate and graduate students, and other computer users in a large academic setting.

Structural equation modeling using partial least squares (PLS-SEM) path coefficients will be used to conduct empirical data analysis to test for main effects, mediation and interaction effects of moderators. Factor analysis will be used to determine the item loadings on the respective constructs thus ensuring content validity of the survey items. Internal consistency tests will also be checked by using cronbach's alpha reliability. VIF test will be performed to ensure that multicollinearity is not an issue. Table-5 shows sample survey items for each construct.

5 CONCLUSION

The purpose of this article is to develop a research model and draw propositions to better understand the pathways through which CT affects CC. Using past literature, we present a model where CA, SEIS and CS are conceptualized as mediators between CT and CC. We also draw key relationships among CA, CS and SEIS in order to increase the explanatory power of the model. Also, CS is modeled as a moderator of the relationship between CA and CC, and between SEIS and CC. The propositions will be tested empirically by administering a survey instrument on computer end users. The use of self-report measurements is a limitation, but such models are difficult to test using other research methods such as experiments. Also, some measures such as compliance are difficult to observe directly.

It is anticipated that the results will demonstrate the importance of the need for technical skills in end-users to improve CC. Literature has emphasized the role of awareness and self-efficacy but has not paid sufficient attention to CS. We believe that while awareness and self-efficacy are important, but their effects will be weak in the absence of technical skills. Our program of research is aimed at testing this belief empirically, and encouraging greater attention to the development of CS among end-users. Our intention is to begin by creating theory-based cybersecurity training materials. These materials will be used to validate the model presented here, and subsequently used to help develop security skills in end-users.

Construct	Sample Survey Item	Response Range
CC	I use anti-spyware software currently. (adapted from Johnston and Warkentin 2010)	Strongly disagree to Strongly Agree
CT	I have received some form of training to protect my computer from attacks. (Self-developed)	Strongly disagree to Strongly Agree
CA	I am aware of the spyware problems and consequences. (Dinev and Hu 2007)	Strongly disagree to Strongly Agree
SEIS	I feel confident handling virus infected files. (Rhee et al. 2009)	No skill to leading performer
CS	I have the skills to detect and remove computer virus and worm (adapted from Choi et al. 2013)	No skill to leading performer

Table-5 Sample Survey Items

REFERENCES

[1] Aytes, K., & Connolly, T. (2005). Computer security and risky computing practices: A rational choice perspective. *Advanced topics in end user computing*, 4, 257.

[2] Bandura, A. (1986). *Social foundations of thought and action* (pp. 5-107). Prentice Hall.: Englewood Cliffs, NJ.

[3] Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review, 84*(2), 191.

[4] Blanke, S. J. (2008). *A Study of the Contributions of Attitude, Computer Security Policy Awareness, and Computer Self-Efficacy to the Employees' Computer Abuse Intention in Business Environments* (Doctoral dissertation, Nova Southeastern University).

[5] Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology, 11*(3-4), 279-295.

[6] Brodie, C. (2008). The importance of security awareness training, https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013 (last visited: Apr 14, 2017)

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

[8] Carlton, M., & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. In *SoutheastCon 2015* (pp. 1-6). IEEE.

[9] Carruth, A. K., Pryor, S., Cormier, C., Bateman, A., Matzke, B., & Gilmore, K. (2010). Evaluation of a School ‐ Based Train ‐ the ‐ Trainer Intervention Program to Teach First Aid and Risk Reduction Among High School Students. *Journal of school health, 80*(9), 453-460.

[10] Cassidy, S., & Eachus, P. (2002). Developing the computer user self-efficacy (CUSE) scale: Investigating the relationship between computer self-efficacy, gender and experience with computers. *Journal of Educational Computing Research*, *26*(2), 133-153.

[11] Choi, M., Levy, Y., & Hovav, A. (2013). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. In *Proc. of the Pre-Int. Conference of Inform. Syst.(ICIS) SIGSEC– Workshop on Inform. Security and Privacy (WISP) 2013.*

[12] Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189-211.

[13] Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly*, 145-158.

[14] Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers & security, 26*(1), 63-72.

[15] Cronan, T. P., Foltz, C. B., & Jones, T. W. (2006). Piracy, computer crime, and IS misuse at the university. *Communications of the ACM, 49*(6), 84-90.

[16] D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20*(1), 79-98.

[17] Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward PIT. *Journal of the Association for Information Systems, 8*(7), 23.

[18] Dworkin, J. B., Larson, R., & Hansen, D. (2003). Adolescents' accounts of growth experiences in youth activities. *Journal of youth and adolescence*, 32(1), 17-26.

[19] Eminagaoglu, M., Ucar, E., and Eren, S. (2009). The positive outcomes of information security awareness training in companies – *A case study, Information Security Technical Report*, 14, 223-229.

[20] Eric Savitz. (2011) (http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/#7e48cb2d31fd, last visited May 4, 2016)

[21] Fischer, K. W. (1980). A theory of cognitive development: The control and construction of hierarchies of skills. *Psychological review, 87*(6), 477.

[22] Foltz, C. B., Paul Cronan, T., & Jones, T. W. (2005). Have you met your organization's computer usage policy?. *Industrial Management & Data Systems, 105*(2), 137-146.

[23] Frayne, C. A., & Latham, G. P. (1987). Application of social learning theory to employee self-management of attendance. *Journal of applied psychology, 72*(3), 387.

[24] Furman, S. M., Theofanos, M. F., Choong, Y. Y., & Stanton, B. (2011). Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, (2), 40-49.

[25] Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. *Journal of applied psychology, 74*(6), 884.

[26] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

[27] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *Management Information Systems, 34*(3), 549-566.

[28] Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

[29] Lerouge, C., Newton, S., & Blanton, J. E. (2005). Exploring the systems analyst skill set: perceptions, preferences, age, and gender. *Journal of Computer Information Systems, 45*(3).

[30] Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

[31] Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems, 11*(7), 394-413.

[32] McCoy, C. (2010). Perceived self-efficacy and technology proficiency in undergraduate college students. *Computers & Education*, *55*(4), 1614-1617.

[33] [33] Marakas, G. M., Yi, M. Y., & Johnson, R. D. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information systems research, 9*(2), 126-163.

[34] Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

[35] NICCS (2015). National initiative for cybersecurity careers and studies. https://niccs.us-cert.gov/awareness/awareness-home

[36] Ozer, E. M., & Bandura, A. (1990). Mechanisms governing empowerment effects: a self-efficacy analysis. *Journal of personality and social psychology, 58*(3), 472.

[37] Potosky, D. (2002). A field study of computer efficacy beliefs as an outcome of training: the role of computer playfulness, computer knowledge, and performance during training. *Computers in Human behavior, 18*(3), 241-255.

[38] Privacy rights website. (http://www.privacyrights.org/data-breach, last visited May 4, 2016)

[39] Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757-778.

[40] Rank, J., Pace, V. L., & Frese, M. (2004). Three avenues for future research on creativity, innovation, and initiative. *Applied Psychology, 53*(4), 518-528.

[41] Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7), 241-253.

[42] Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

[43] SANS Institute. (2001) (https://www.sans.org/reading-room/whitepapers/vpns/weakest-link-human-factor-lessons-learned-german-wwii-enigma-cryptosystem-738, last visited May 4, 2016)

[44] [44] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

[45] Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy CC: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42-75.

[46] Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

[47] Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 441-469.

[48] Torkzadeh, G., & Lee, J. (2003). Measures of perceived end-user computing skills. *Information & Management, 40*(7), 607-615.

[49] Torkzadeh, G., & Van Dyke, T. P. (2002). Effects of training on Internet self-efficacy and computer user attitudes. *Computers in Human Behavior, 18*(5), 479-494.

[50] Torkzadeh, G., Chang, J. C. J., & Demirhan, D. (2006). A contingency model of computer and Internet self-efficacy. *Information & Management, 43*(4), 541-550.

[51] Torkzadeh, R., Pflughoeft, K., & Hall, L. (1999). Computer self-efficacy, training effectiveness and user attitudes: An empirical study. *Behaviour & Information Technology, 18*(4), 299-309.

[52] Udo, G. J., Bagchi, K. K., & Kirs, P. J. (2010). An assessment of customers' e-service quality perception, satisfaction and intention. *International Journal of Information Management, 30*(6), 481-492.

[53] Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586.

[54] Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs, 61*(2), 113-134.