International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 16, Issue 2, 2022

Predicting Computer Self-Efficacy of E-Learning Systems Security Attacks using Confirmatory factor Analysis

Fahad M Alsaadi, Taif University, Email: fmsaadi@tu.edu.sa

Since many academic institutions in US have adopted e-learning systems to facilitate collaboration among the students and their professors, demand has been created to assess the perceptions of Saudi students on the severity of the unethical actions in attacks to the e-learning system. This study investigated the prediction relationship between the Computer Self-Efficacy (CSE), and Students Computer Skills (SCS), Security of E-learning Systems (SOM), Resistance to using e-learning system (RTU) and IS Usage (ISU), as well as predicting the relationship between Security of E-learning Systems (SOM) and Students Computer Skills (SCS) on the severity of the unethical actions in attacks to the e-learning system based on Saudi students' perspective. Confirmatory Factor Analysis (CFA) and Structural Equations Modeling (SEM) have been performed using SmartPLS software. Cronbach's Alpha results for each factor demonstrates reliability for all constructs measured.

Keywords: *Computer Self-Efficacy, e-learning systems security, Confirmatory factor Analysis*

Introduction

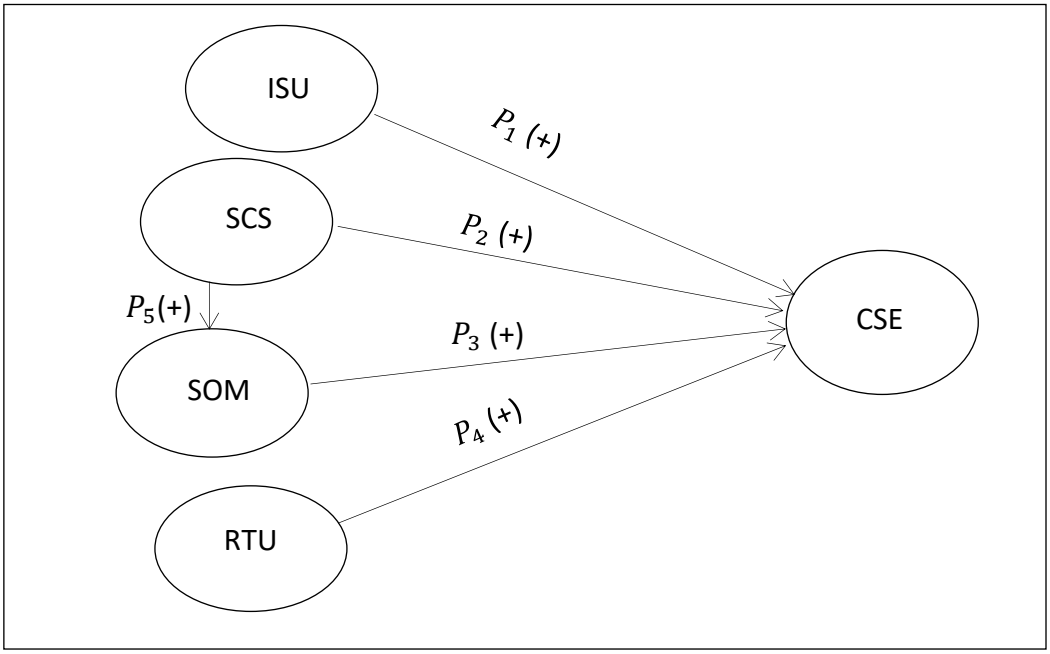
The significant growth of online learning at higher educational institutions around the world remains at record high (Anastasiades, Vitalaki, & Gertzakis, 2008; Littlejohn, Falconer, & McGill, 2008; Shee & Wang, 2008). Scholars have discussed the increase in the seriousness of unethical behaviors taken into account the management of information system field (Jalal, Zeb, 2016). These unethical behaviors include cyber-attacks beside the issue of identity theft, which would impact the education system of countries adversely (Tagert, 2010). Other scholars have illustrated the levels of authentication strength perceived by users in terms of e-learning systems (Beaudin, 2016). Some information systems (IS) scholars became interested in investigating and controlling these

breaches (Tagert, 2010). In addition, research has shown that students engaging in misconduct in their academic career and are more likely to engage in unethical behavior during their professional career (Levy, Ramim, & Hackney, 2013). Therefore, many IS scholars have shifted their attention to investigating the legal requirements of ethics (Tagert, 2010). Nevertheless, little consideration has been given to exploring and understanding the ethical severity of cyber-attacks alongside unethical behavior in academic institutions. As many institutes are moving towards embracing the use of e-learning systems, the students may be more likely to engage in unethical behavior through such systems (Leonard, Cronan, Kreie, 2003). It becomes a necessity for the students to be aware of any IS breaches through the e-learning systems (Yunus, Zumzuri, 2013). This information will help in establishing the learners' understanding of e-learning cyber-attacks as the educated have more capability to manage security threats (Rabai, Ben Aissa, 2012). Therefore, this paper was aimed at measuring perception of Saudi students as they fully meet the criteria for the determination of the severity of the unethical actions in the e-learning systems. Saudi Students were chosen for this study, because Saudi Arabia is one of the growing countries in terms of using e-learning systems, and most of Saudi students have lack of awareness of the security issues in the e-learning systems.

Research Questions

RQ1: To what extend can the Information Security Usage (ISU) predict the Computer Self-Efficacy (CSE).
RQ2: To what extend can the Students Computer Skills (SCS) predict the Computer Self-Efficacy (CSE).
RQ3: To what extend can the Security of E-learning Systems (SOM) predict the Computer Self-Efficacy (CSE).
RQ4: To what extend can the Resistance to using e-learning system (RTU) predict the Computer Self-Efficacy (CSE).
RQ5: To what extend can the Students Computer Skills (SCS) predict the Security of E-learning Systems (SOM).

Figure 1: The Conceptual Research Map (N=131)



Methodology

This study targeted 131 Saudi students both male and female at the undergraduate and graduate level during their time studying at US universities. A quantitative survey instrument was developed by using survey items from the following prior validated instruments: Students Computer Skills (SCS) (Torkzadeh & Lee, 2003), Computer Self-Efficacy (CSE) (Levy & Green, 2009), Security of E-learning Systems (SOM) (Levy, Ramim, & Hackney, 2013), Resistance to Using e-learning system (RTU) (Levy & Danet 2010) and Information Security Usage (ISU) (Levy & Danet 2010).

Propositions

P1: Information Security Usage (ISU) will demonstrate a positive significant contribution in predicting Computer Self-Efficacy (CSE).
P2: Students Computer Skills (SCS) will demonstrate a positive significant contribution in predicting the classification of Computer Self-Efficacy (CSE).
P3: Security of E-learning Systems (SOM) will demonstrate a positive significant contribution in predicting Computer Self-Efficacy (CSE).
P4: Resistance to using e-learning system (RTU) will demonstrate a positive significant contribution in predicting Computer Self-Efficacy (CSE).
P5: Students Computer Skills (SCS) will demonstrate a positive significant contribution in predicting Security of E-learning Systems (SOM).

Analysis Done

This study aimed 131 Saudi students from different universities including public and private universities in USA. This study examined four independent variables: ISU, SCS, SOM, and RTU and their contribution to the dependent variables: CSE, and SOM.

The researchers started by preforming data screening including frequencies, descriptive statistics and multivariate outliers using the Mahalanbois Distance test. Then, a Multivariate Normality Next applied to see weather the data is normally distributed or not. Also, correlation test between all IVs and DVs that noted in the research questions and propositions were applied and the results are shown under the result section.

After the researchers have preformed pre-analysis data screening including multivariate outliers (using Mahalanobis Distance), they have performed Confirmatory Factor Analysis (CFA) and Structural Equations Modeling (SEM) using SmartPLS.

Results

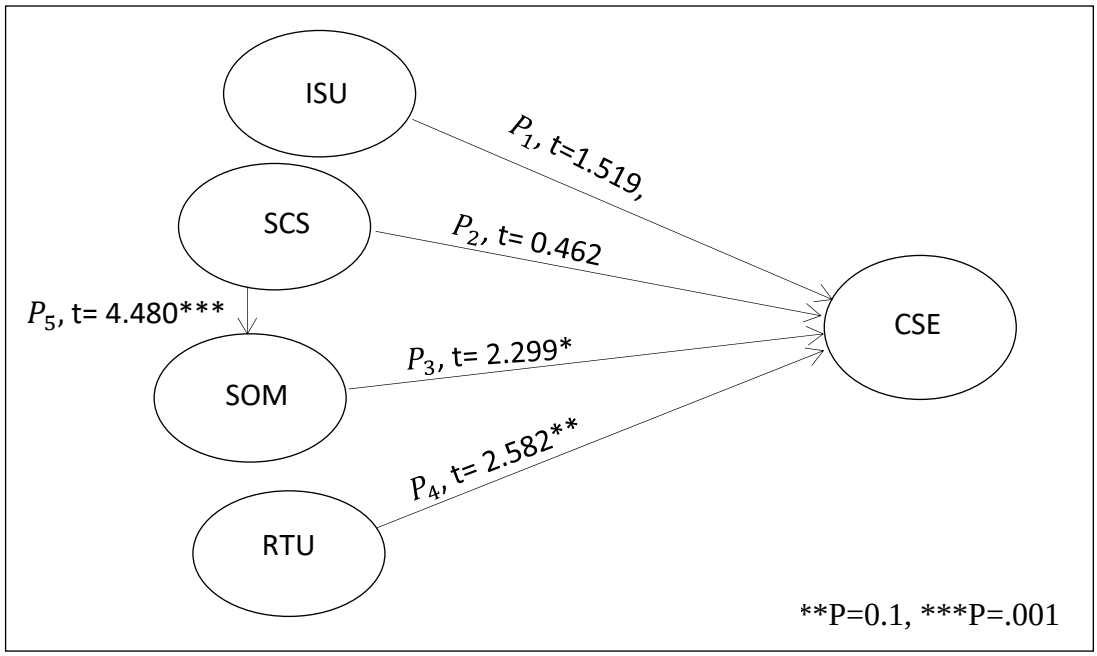
Smart PLS test was conducted to figure out whether there is a significant contribution between the independent variables (ISU, RTU, SOM, and SCS) and the dependent variables (CSE and SOM). The model predictive power was tested through R^2 value for CSE is 0.43 which is below the moderate level 0.50; and the R^2 value for SOM is 0.17 which is below the weakness level 0.25, The model predictability power was not substantial enough (below 0.75) to be generalized based on the given R square values (R^2s) for the dependents variables.

Reliability estimates were calculated for each construct using Cronbach's Alpha analysis. Research indicates that Cronbach Alpha of over .70 represents a reliable factor (Kettinger & Lee, 1994). The Cronbach's Alpha for CSE, ISU, RTU, SCS, SOM, where 0.93, 0.82, 0.88, 0.91, 0.86 respectfully demonstrating high reliability for all construct measures. Table 1 shows the summary of each construct's Cronbach's Alpha.

Table 1: Summary of Each Construct's Cronbach's Alpha (N=131)

Constructs Name	Cronbachs Alpha
CSE	0.934
ISU	0.828
TRU	0.886
SCS	0.916
SOM	0.862

Figure 2: Results of PLS Analysis (N=131)



Result of the PLS analysis indicated that SCS has the strongest significant impact on SOM (when T-Value is 4.480, the P-Value is < .0001). Also SOM and RTU have significant impacts on CSE (as T-Value is 2.299, the P-Value is 0.012 while when T-Value is 2.582, the P-Value is .005. The result is significant at p < .05.). Whereas SCS and ISU have no significant impact on CSE (as T-Value 0.462, The P-Value is .322, The result is not significant while when T-Value is 1.519, the relationship is significant at a P-Value is .0656, the result is *not* significant at p < .05); which means that the researchers failed to reject P3, P4, and P5 while they rejected P3 and P2.

Conclusion and Discussion

This study is conducted to find the Saudi students' perceptions of ethical severity related to security attacks in the e-learning environment. The aim of this study was to predict the dependent variables of this study including Computer Self-Efficacy (CSE), and Security of E-learning Systems (SOM), toward the other independent variables including Students Computer Skills (SCS), Security of E-learning Systems (SOM), Resistance to using e-learning system (RTU), and Information Security Usage (ISU) to figure out their impact on the severity of the unethical actions in attacks to the e-learning system based on Saudi students perspective.

The main limitation that can be observed in this study is that most of Saudi students are inexperienced enough to asset their observation about e-learning systems security attacks, although it's one of the most growing countries in e-learning systems (Alkhalaf, Ngyuen, Drew 2010).

Future research in this area would be the influence that security attacks has on the progress of students that lack security skills.

References

Anastasiades, P. S., Vitalaki, E., & Gertzakis, N. (2008). Collaborative learning activities at a distance via interactive videoconferencing in elementary schools: Parents' attitudes. Computers & Education, 50(4), 1527–1539.

Alkhalaf, S., Nguyen, A., & Drew, S. (2010). Assessing eLearning Systems in the Kingdom of Saudi Arabia's Higher Education Sector.

Beaudin, S. (2016). An Empirical Study of Authentication Methods to Secure E-learning System Activities Against Impersonation Fraud.

Bandara, I., Ioras, F., & MaherI, K. (2014, November). Cyber Security Concerns in E-Learning Education. In *Proceedings of ICERI2014 Conference*, *17th-19th November*.

Kettinger, W. J., & Lee, C. C. (1994). Perceived service quality and user satisfaction with the information systems. Decision Sciences, 25(5/6), 737–767.

Levy, Y., Ramim, M. M., & Hackney, R. A. (2013). Assessing ethical severity of e-learningsystems security attacks. *Journal of Computer Information Systems*, *53*(3), 75-84.

Levy, Y., & Danet, T. L. (2012). Implementation Success Model in Government Agencies: A Case of. *Advancing the Service Sector with Evolving Technologies: Techniques and Principles: Techniques and Principles*, 105.

Leonard, L. N., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management*, *42*(1), 143-158.

Liaw, S. S. (2008). Investigating students' perceived satisfaction, behavioral intention, and effectiveness of e-learning: A case study of the Blackboard system. *Computers & Education*, *51*(2), 864-873.

Liu, X., Liu, S., Lee, S., & Magjuka, R. J. (2010). Cultural differences in online learning: International student perceptions. *Educational Technology & Society*, *13*(3), 177-188.

Mertler, C. A., & Vannatta, R. A. (2002). Advanced and multivariate statistical methods. *Los Angeles, CA: Pyrczak*.

Tagert, A. C. (2010). Cybersecurity challenges in developing nations. Pittsburgh, PA: CarnegiMellon University.

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

Jalal, A., & Zeb, M. A. (2008). Security enhancement for e-learning portal. *International Journal of Computer Science and Network Security*, *8*(3), 41-45.