



## Determining the effects of information security knowledge on information security awareness via structural equation modelings

Sinan Saraçlı\*<sup>†</sup>  and Atilgan Erdoğan<sup>‡</sup> 

### Abstract

The aim of this study is by investigating the Information Security Awareness of University Students via statistical techniques, revealing the existing awareness and giving some suggestions to improve this awareness. By the internet, which entered our daily life rapidly, information and technology era has been started and it gave new point of view by changing our lifestyle in many areas as electronic commerce, education and government. By developing and rapidly improving technology, Individuals' having enough capacity to use it, information culture has spread over all parts of the society. By increasing the information systems and internet every day, by using private and secret information, doing both public and individual processes via these systems has increased the importance of information and information systems and resolve the information awareness as an obligatory case. It can be observed nowadays that there are many information guilt is being perpetrated. Its known that related ministry in our country is taking enough security precautions both hardware and software for the information and system security and researching on new actions. However, the most important factor to pan out for the information and system security is the development of corporate and individual awareness. With this purpose, to measure the computer usage praxis and Information Security Awareness levels of Students of Afyon Kocatepe University, by using "Information Security Awareness Scale", which has developed previously the related data is obtained via a questionnaire and analyzed by SPSS and LISREL software. In this study as statistical techniques, Explanatory Factor Analysis, Confirmatory Factor Analyzes and Structural Equation Modeling is used.

**Keywords:** Information security, Security awareness, Structural equation modeling.

*Mathematics Subject Classification (2010):* 2010 AMS Classification: 62J99, 62-09, 62H99, 62-07, 62J12.

*Received :* 13.06.2018 *Accepted :* 10.09.2018 *Doi :* 10.15672/HJMS.2018.641

---

\*Afyon Kocatepe University, Faculty of Science, Department of Statistics, 03200 Afyonkarahisar, TURKEY, Email: [ssaracli@aku.edu.tr](mailto:ssaracli@aku.edu.tr)

<sup>†</sup>Corresponding Author.

<sup>‡</sup>Prime ministry, data processing department, Ankara, TURKEY. This study is a part of Atilgan Erdogmuss MS thesis supervised by Sinan Saracli at Afyon Kocatepe University Institute of Science, and it is founded by Afyon Kocatepe University, Scientific Research Project Council. Project No: 16. KARIYER.125 and a part of this study is presented at 9th International Conference on Social Science and Humanities, Bangkok, Thailand., Email: [atilgun@gmail.com](mailto:atilgun@gmail.com)

## 1. Introduction

As a result of improvements in information technology, central bodies have been replaced by scattered architectural designs, and electronic applications that are accessible through internet and network. Several concepts beginning with e- (e-commerce, e-education, e-reservation, e-exam, e-school, ebank, etc.) have been become a part of our life as a consequence of an increase in using of electronic information infrastructures, for instance internet, computer networks, online systems, remote access and so on [22].

Awareness and behavior among all kinds of users are important parts of the information security performance of an organization. Adequate information security training is thus required in order to create and improve user awareness and behavior. This paper discusses and evaluates the effects of a training programme aimed at improving users information security awareness and behavior by involving them directly. Several single or combined measures might be taken in order to improve users information security performance [7, 23], ranging from the distribution of messages via, e.g. pamphlets, e-mails, intranet pages, screen savers, posters, mouse pads, and pens to games, formal presentations, lunch meetings, and training courses [2].

Most IS security managers pay more attention to technical issues and solutions such as firewalls, routers, and intrusion detection software, while pay less focus on soft issues such as the hazards caused by end users lack of IS security awareness [9]. Information security awareness can be described as a state where users in an organization are aware of their security mission [20, 16].

Cyber threats increase continuously with the introduction of new technologies and the legal boundaries related to the privacy of personal information and its use by the corporations are not clear and are often subject to legal interpretation. Consequently, it is an obligation of the person to be aware of the threats and to protect his or her personal information. However, due to inappropriate use of technology and since individuals level of awareness toward threats on information security is low, significant information security risks do exist. Therefore, with the aim of achieving higher information security, numerous software and hardware protection methods have been developed, making it quite hard to exploit information systems (IS) in terms of software and hardware gaps. Despite these high investments, as stated by Pahlila et al.[13], the number of security incidents does not decrease. Abawajy [1] points out that no matter how many and how strong the layers of technological defenses in an organization, the information security is only as strong as its weakest link, and different tools, such as social engineering, can be used to target individuals, who can be considered to be the weakest link of the security chain [3, 8, 19, 25]. Stanton et al. [21] concisely address this by stating that even the best technology that can be used to mitigate numerous IS security problems cannot work successfully unless the people in organizations do the right thing [12].

Students (aged 18-24 year olds) are high-risk and attractive candidates for security attacks. This can be explained by the fact that students are typically transient and have less credit history than more established adults [11]. A student may receive a web postcard in an email, and inadvertently installs a Trojan horse onto his system, becoming a victim of a clever social engineering attack [11, 16].

## 2. Method

Structural Equation Model (SEM) is a method for representing, estimating and testing a theoretical network of linear relations between variables [17]. The structural model is that component of general model that prescribes relations between latent variables and observed variables that are not indicators of latent variables. SEM is a statistical technique for testing and estimating causal relationships using a combination of statistical

data and qualitative causal assumptions. It is used in social, behavioral and educational sciences, namely, psychology, biology, economy, marketing and medicine.

SEM is a comprehensive statistical method used in testing hypotheses about causal relationships among observed and unobserved (latent) variables and has proved useful in solving the problems in formulating theoretical constructions [15]. Its function has found to be better than other multivariate statistics techniques which include multiple regression, path analysis and factor analysis. Other statistics techniques could not take them into consideration due to the interaction effects among depend and independent variables. Therefore, a method that can examine a series of dependence relationships simultaneously helps to address complicated managerial and behavioral issues. SEM also can expand the explanatory ability and statistical efficiency for model testing with a single comprehensive method [14, 24]. As the assumptions of structural models, five general conditions must met before one can reasonably infer a causal relation between two variables [10]:

The presumed cause (e.g., X) must occur before the presumed effect (e.g., Y); that is, there is temporal precedence.

There is association, or an observed covariation, between X and Y.

There is isolation, which means that there are no other plausible explanations (e.g., extraneous or confounding variables) of the covariation between X and Y; that is, their statistical association holds controlling for other variables that may also effect Y.

The form of the distribution of the data is known; that is, the observed distributions match those assumed by the method used to estimate associations.

The direction of the causal relation is correctly specified; that is, X indeed causes Y instead of the reverse, or X and Y cause each other in a reciprocal manner.

### 3. Sample and Scale

In terms of sampling theory, since the general proportion of the attitudes and behaviors of the population within the frame of research was not obvious, the contingent sampling technique could not be applicable. Assuming the normality assumption is met, the method that grounds on the acceptable error level was used in determining the volume of the sample. In the equation, which is calculated by using the formula indicating that the number of units to which the scale is carried out,  $n = \{(z^2)(\sigma^2)\}/(d^2)$ ; the volume of sample was calculated as 500; on 0.05 significant level,  $z = 1.96$   $d(\text{sensitivity}) = 0.043$ , p and q values as 0.5. After determining sampling, a 5-point Likert-type questionnaire ranging from 1 (definitely disagree) to 5 (definitely agree) is applied to randomly 560 students in the campus of Afyon Kocatepe University between dates 1-30 November, 2016. Because of some unfilled and wrong replied questionnaires, analyzes are concluded over 546 questionnaires via SPSS and LISREL software.

### 4. Findings

Before applying the SEM, as a statistical order, Explanatory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) applied to related data set. The results of EFA and Cronbachs  $\alpha$  values for the factors A, B, C, D and E are given in Table 1.

**Table 1.** EFA Results and Cronbachs Alpha values for the factors A, B, C, D and E.

Factors/Items	Factor Loading	Eigen value	Explained Variance (%)	Cronbachs Alpha
<b>A. Internet security</b>				
A1. I am aware of the effects, if a malware is infected in my device.	.748			
A2. I am aware of not to click on the links that I dont know, otherwise a malware may infect device when I am surfing.	.719			
A3. I am aware not to apply any online banking and online shopping from any network that I have a suspicion about its security.	.621	1.753	12.884	.730
A4. I am aware not to apply any online banking and online shopping from any device that is not my own.	.602			
A5. I am aware that it's important for my information security to use different passwords for each account and application that I use online	.518			
<b>B. Social Network Usage</b>				
B1. I am aware that accepting a friend request from an unknown user in social media that may cause a security flaw.	.773			
B2. I am aware that an open fireball to everyone in social media may cause a security problem.	.828	4.894	14.011	.785
B3. I am aware that my personal pictures that I shared in social media may be used in bad faith.	.718			
B4. I am aware that sharing the location information in social media may cause a security problem.	.694			
<b>C. Web browser and Network Security</b>				
C1. I am aware that is recorded in cookies, how much time I spend in which website.	.698			
C2. I am aware that my information can be followed by packed users from any network that I connected.	.735	1.416	10.754	.682
C3. I am aware that I may be routed to any fake websites even if I entered the correct website name.	.720			
<b>D. Password Generation</b>				
D1. I am aware of not using last five passwords and changing it every month is important for information security.	.654			
D2. I am aware of generating a strong (complex and long) password, may increase my security.	.672	1.171	10.099	.569
D3. I am aware of not to use any personal information about me inside of my passwords and it should be complex.	.701			
<b>E. Social Media Traps</b>				
E1. I am aware that when I connect to some social networks, my location information can be seen	.573			
E2. I am aware that that applications that I use through social networks can share my information without my permission.	.827	1.058	9.428	.631
E3. I am aware that my user information in application software may be sold to any companies with the intend of questionnaire, advertisement and marketing.	.705			

As a result of the EFA, there are 5 factors for general information security awareness named as A: Internet security, B: Social Media Usage, C: Web browser and Network Security, D: Password Generation and E: Social Media Traps explained the 57.177 % of total variance and total Cronbachs alpha values for these five factors is calculated as 0.839.

**Table 2.** EFA Results and Cronbachs Alpha values for the factors Threats and Precautions.

Factors/Items	Factor Loading	Eigen value	Explained Variance (%)	Cronbachs Alpha
<b>X. Threats</b>				
ISAX1. I know what is fake virus protection software	.812			
ISAX2. I know taking measure about the security precautions for id robbery.	.795			
ISAX3. I know precaution methods for spywares	.764			
ISAX4. I know taking measure about the security precautions for malwares.	.722	6.343	32.385	.887
ISAX5. I know how to act, not to exposure a social engineering attack.	.651			
ISAX6. I can understand whether there is a spyware in my computer or not.	.630			
ISAX7. I can understand whether a malicious code is involved in my computer or not.	.612			
<b>Y. Precautions</b>				
ISAY1. I know how to use the virus protection software in information systems.	.822			
ISAY2. I know about the points to consider to keep the physical security for the portable devices.	.786			
ISAY3. I use real-time protection feature of my virus protection software in my computer.	.725	1.259	26.092	.835
ISAY4. I know about the points to consider when I use the USB drives.	.577			
ISAY5. I know about the points about data security for the portable devices.	.582			
ISAY6. I know how to make an automatic update for my virus protection software in my computer.	.522			

According to EFA results 2 factors named as X: Threats and Y: Precautions related with Information Security Awareness (ISAX and ISAY) explains the 58.478 % of total variance and total Cronbachs alpha values for these two factors is calculated as 0.912.

Related with these EFA results, CFA is applied to this data set and results are given in Figure 1 and Figure 2. For CFA and SEM, to improve the fitness of the model, there has also some modifications applied by suggestions of the software, by adding some error covariances to the variables.

There are more than one goodness of fit index for CFA and SEM. The most commonly used test statistics in SEM are likelihood ratio chi-square statistics ( $X^2$ ), root mean square error of approximation statistics (RMSEA), goodness of fit index statistics (GFI) and adjusted goodness of fit index statistics (AGFI).

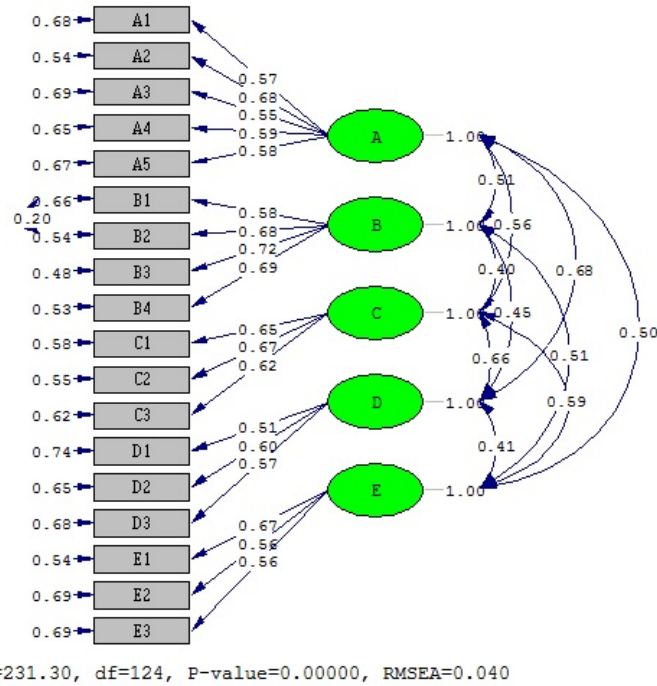


Figure 1. CFA Results for the factors A, B, C, D and E.

Table 3, shows that the Structural Model given in Figure 1 is statistically significant and has a good fitness according to all goodness of fit statistics. Besides these Fitness Criteria  $X^2(124) = 231.30$ ;  $X^2/df = 1.865 < 3$  also means that there is an acceptable fit.

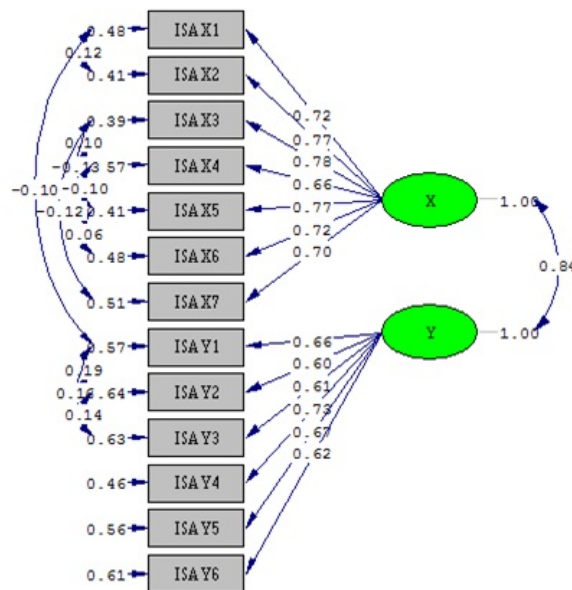
Table 3. Limits and the results of the structural model.

Fitness Criterion	Perfect Fitness	Acceptable Fitness	ABCDE	XY	X	Y
RMSEA	$0 < RMSEA < 0.05$	$0.05 \leq RMSEA \leq 0.10$	0.040	0.058	0.048	0.045
NFI	$0.95 \leq NFI \leq 1$	$0.90 < NFI \leq 0.95$	0.95	0.98	0.93	0.94
NNFI	$0.97 \leq NNFI \leq 1$	$0.95 \leq NNFI \leq 0.97$	0.97	0.98	0.95	0.96
CFI	$0.97 \leq CFI \leq 1$	$0.95 \leq CFI \leq 0.97$	0.98	0.99	0.96	0.96
SRMR	$0 \leq SRMR < 0.05$	$0.05 \leq SRMR \leq 0.10$	0.038	0.035	0.081	0.069
GFI	$0.95 \leq GFI \leq 1$	$0.90 \leq GFI \leq 0.95$	0.95	0.96	0.92	0.93
AGFI	$0.90 \leq AGFI \leq 1$	$0.85 \leq AGFI \leq 0.90$	0.94	0.93	0.90	0.91

(Source: [18] RMSEA: Root Mean Square Error of Approximation, NFI: Normed Fit Index, NNFI: Non-Normed Fit Index, CFI: Comparative Fit Index, SRMR: Standardized Root Mean Square Residual, GFI: Goodness of Fit Index, AGFI: Adjusted Goodness of Fit Index)

For the sub-factors of Information security, named as : (A) Internet security, (B) Social Media Usage, (C) Web browser and Network Security, (D) Password Generation and (E) Social Media Traps, the results of CFA, given in Figure 1 indicate that, the most important variables on these factors are A2. "I am aware of not to click on the links that I dont know, otherwise a malware may infect device when I am surfing", B3. I am aware that my personal pictures that I shared in social media may be used in bad

faith. C2. I am aware that my information can be followed by packed users from any network that I connected. D2. I am aware of generating a strong (complex and long) password, may increase my security and E1 "I am aware that when I connect to some social networks, my location information can be seen" with the coefficients of 0.68, 0.72, 0.67, 0.60 and 0.67 respectively. The results also indicate that among these sub-factors while the highest correlation is between Internet security and Password Generation with the coefficient of 0.68, the lowest correlation is between Social Media Usage and Web browser and Network Security with the coefficient of 0.40.

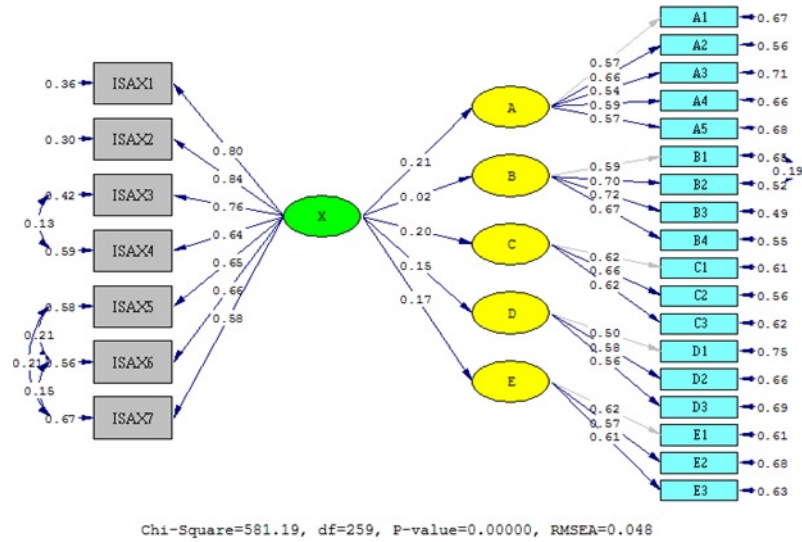


Chi-Square=153.55, df=54, P-value=0.00000, RMSEA=0.058

**Figure 2.** CFA Results for the factors X and Y.

According to all goodness of fit statistics, given in Table 3, the Model given in Figure 2 is also statistically significant. Besides for this model  $X^2(54) = 153.55$ ;  $X^2/df = 2.843 < 3$  is also another indicator to an accept this model statistically significant.

According to results of CFA, given in Figure 2., for Threats (X) and Precautions (Y) which are the sub factors of general security information, the most important variable on the students information about Threats is ISAX3: "I know precaution methods for spywares" with the coefficient of 0.78. the most important variable on these students information about precautions is ISAY4: "I know about the points to consider when I use the USB drives" with the coefficient of 0.73. The results also indicate that there is a positive and strong correlation between the information of Threats and precautions with the coefficient of 0.84. Considering the EFA and CFA results, to determine the relations among the students information about Threats and sub-factors of information security awareness, the results of SEM is given in Figure 3. and for this model the alternative research hypotheses are given in Table 4.



**Figure 3.** Structural model for student’s information about threats and awareness about the sub factors of information security.

**Table 4.** Alternative Study Hypotheses

Hypotheses
$H_1$ As the students information about Threats increases, their Internet security awareness increases.
$H_2$ As the students information about Threats increases, their Social Media Usage awareness increases.
$H_3$ As the students information about Threats increases, their Web browser and Network Security awareness increases.
$H_4$ As the students information about Threats increases, their Password Generation awareness increases.
$H_5$ As the students information about Threats increases, their Social Media Traps awareness increases.

According to all goodness of fit statistics, given in Table 3, the Structural Model given in Figure 2 is within the acceptable limits and for this model  $X^2(259) = 581.19$ ;  $X^2/df = 2.244 < 3$  means statistically significant too.

As it can be seen from Figure 3., on the information about threats, the most and the less important sub-factors of information security awareness are Internet security awareness and Password Generation awareness respectively. Because the path from threats to social media usage is not statistically significant as given in Table 5., the coefficient of this path is ignored. According to other coefficients it can be said that for the one unit increase on the students’ information about threats there will be 0.21 unit increase for their awareness about Internet security, 0.20 unit increase for their awareness about Web browser and Network Security, 0.17 unit increase for their awareness about Social Media Traps and 0.15 unit increase for their awareness about password generation. Results of the hypothesis tests for the structural model given in Figure 3 are given in Table 5.



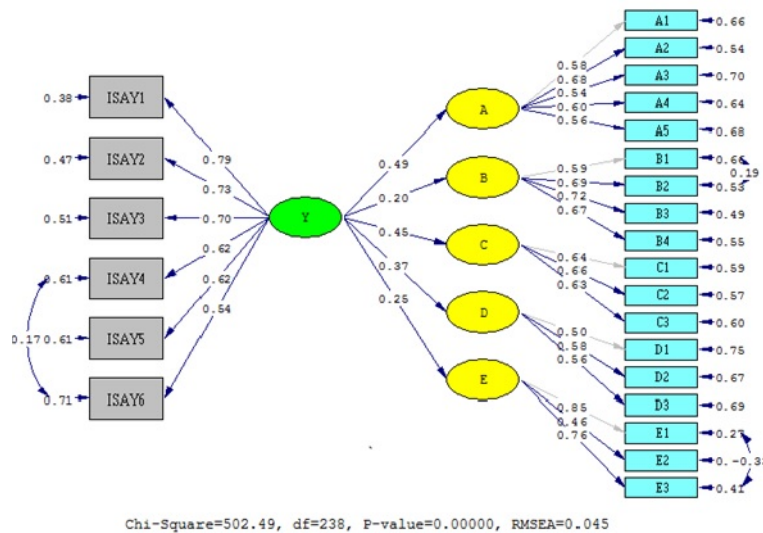
**Table 5.** Standardized parameter estimate values, t values and hypotheses for the model given in Figure 1.

Hypotheses	Paths	Standardized parameter estimate values	t values	Results
$H_1$	$(X) \rightarrow (A)$	0.21	3.88	Confirmed
$H_2$	$(X) \rightarrow (B)$	0.02	0.43	Not Confirmed
$H_3$	$(X) \rightarrow (C)$	0.20	3.49	Confirmed
$H_4$	$(X) \rightarrow (D)$	0.15	2.36	Confirmed
$H_5$	$(Y) \rightarrow (E)$	0.17	2.89	Confirmed

As it can be seen from Table 3. except  $H_2$ , all the hypotheses about this Structural Model are confirmed. To determine the relations among the students information about Precautions and sub-factors of information security awareness, the results of SEM is given in Figure 4. The alternative research hypotheses for this model are also given in Table 6.

**Table 6.** Alternative Study Hypotheses

Alternative Hypotheses
$H_6$ As the students information about Precautions increases, their Internet security awareness increases.
$H_7$ As the students information about Precautions increases, their Social Media Usage awareness increases.
$H_8$ As the students information about Precautions increases, their Web browser and Network Security awareness increases.
$H_9$ As the students information about Precautions increases, their Password Generation awareness increases.
$H_{10}$ As the students information about Precautions increases, their Social Media Traps awareness increases.



**Figure 4.** Structural Model for student’s information about Precautions and awareness about the sub factors of information security.

For the Structural Model given in Figure 4,  $X^2(238) = 502.49$ ;  $X^2/df = 2.111 < 3$  and all the goodness of fit statistics, given in Table 2 are within the acceptable limits for this model.

Results of Structural Equation modeling given in Figure 4., indicate that on the information about precautions, the most and the less important sub-factors of information security awareness are Internet security awareness and social media usage awareness respectively. Figure 4 also indicate that for the one unit increase on the students' information about precautions there will be 0.49 unit increase for their awareness about Internet security, 0.45 unit increase for their awareness about Web browser and Network Security, 0.37 unit increase for their awareness about password generation, 0.25 unit increase for their awareness about Social Media Traps and 0.20 unit increase for their awareness about Social Media Usage.

Results of the hypothesis tests for the structural model given in Figure 4 are given in Table 7.

**Table 7.** Standardized parameter estimate values, t values and hypotheses for the model given in Figure 2.

Hypotheses	Paths	Standardized parameter estimate values	t values	Results
$H_1$	$(Y) \rightarrow (A)$	0.49	8.17	Confirmed
$H_2$	$(Y) \rightarrow (B)$	0.20	3.66	Confirmed
$H_3$	$(Y) \rightarrow (C)$	0.45	7.55	Confirmed
$H_4$	$(Y) \rightarrow (D)$	0.37	5.36	Confirmed
$H_5$	$(Y) \rightarrow (E)$	0.25	5.26	Confirmed

As it can be seen from Table 7. all of the hypotheses about this Structural Model are confirmed.

## 5. Results and Discussion

There are many studies on information security and they all mention the importance of threats and the precautions to be more secure in this digital era. In this study the effects of threats and precautions on the awareness of information security is examined separately via structural equation modeling. As a result within the threats as information security knowledge, the most effective factor found as knowledge on taking measure about the security precautions for ID robbery (ISAX2). Edgeways, knowledge about Threats most effect internet security as the sub-factor of information security awareness. Within internet security awareness, the most effective factor is found as being aware of not to click on the links that he/she doesnt know, otherwise a malware may infect device when they are surfing (A2).

This results also corresponds with the results of [4]. In their research on the main factors of information security, they found that some malevolent people make some information robbery via using the sore points of the systems and getting personal and corporate information. As a precaution they also mentioned the importance of checking and controlling these kinds of software continuously.

Similarly, in another study, Gökmen and Akgün [6] mentioned that in recent years one of the most important attacks towards information systems is forwarding the users to fake web sites by fishing. By this way malevolent people get the bank accounts, e-mail and social media accounts of the people who are unaware of information security.

In their study Çakır and Kesler [5] mentioned the importance of not to click on the links which the users are not completely sure. This result also corresponds with the result of our study. In our study, we found that the awareness on clicking the unknown links while surfing is the most effective variable on internet security awareness. Importance of using anti-virus software is also the common result as getting some precautions.

One of the other results of this study by considering the effects of information security knowledge about precautions on the information security awareness is; within the precaution knowledge, the most effective factor found as knowing how to use the virus protection software in information systems (ISAY1). Effect of precautions again shows itself much on internet security as the sub-factor of information security awareness and again within internet security awareness, the most effective factor is found as being aware of not to click on the links that he/she doesn't know, otherwise a malware may infect device when they are surfing (A2).

Besides other studies, the results of this study also correspond itself and internet security becomes the most important factor to be considered among all other factors. Combining with the other factors if it is not considered and supported with other useful tools, people may be in trouble both from economical and spiritual sides.

Additively to the results of this study, to improve the information security awareness, people should be warned and much educated about spywares, points to consider when using the USB drives, generating a strong (complex and long) password, being careful for sharing location information, being careful when connecting the internet from an unknown network, being careful while sharing personal picture.

**Acknowledgement:** This study is a part of Atılğan Erdoğan's MS thesis supervised by Sinan Saraçlı at Afyon Kocatepe University Institute of Science, and it is founded by Afyon Kocatepe University, Scientific Research Project Council. Project No: 16. KARIYER.125 and a part of this study is presented at 9th International Conference on Social Science and Humanities, Bangkok, Thailand. The authors would like to thank to Afyon Kocatepe University, Scientific Research Project Council for their support.

## References

- [1] J. Abawajy. User preference of cyber security awareness delivery methods, *Behav Inf Technol* 33(3), 237-248, 2014.
- [2] E. Albrechtsen and J. Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study, *Computers & Security*, 29, 432-445, 2010.
- [3] I. Arce. The weakest link revisited, *IEEE Secur Priv* 1(2), 72-6, 2003.
- [4] G. Canbek ve S. Sagiroglu. Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme, *Politeknik Dergisi* 9(3), 165-174, 2006.
- [5] S. Çakır ve M. Kesler. Bilgisayar Güvenliğini Tehdit Eden Virüsler ve Antivirüs Yazılımlar, XIV. Akademik Biliim Konferans, 551-558, 1-3ubat, 2012.
- [6] O.F. Gökmen ve O.E. Akgün. Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi, *İlköğretim Online*, 14(4), 1208-1221, 2015.
- [7] W. Hubbard. Methods and techniques of implementing a security awareness program, SANS Institute, white paper, 2002.
- [8] K. Jansson and R. Von Solms. Phishing for phishing awareness, *Behav Inf Technol.*, 32(6), 584-593, 2013.
- [9] F.H. Katz. The effect of a university information security survey on instructing methods in information security, In: *Proceedings of the second annual conference on information security curriculum development*, 43-48, 2005.
- [10] R.B. Kline. Assumptions in structural equation modeling, In R.H. Hoyle (Ed.), *Handbook of structural equation modeling*, 111-125, New York, US:Guilford Press, 2010.

- [11] A. Marks. Exploring universities information systems security awareness in a changing higher education environment: a comparative case study research, PhD thesis, University of Salford, 2007.
- [12] G. Ogutcu, O.M. Testik and O. Chouseinoglou. Analysis of personal information security behavior and awareness, *Computers & Security*, 56, 83-93, 2016.
- [13] S. Pahnla, M. Siponen and A. Mahmood. Employees behavior towards IS security policy compliance, In: 40th Annual Hawaii International Conference on System Sciences, HICSS 2007. IEEE; 2007.
- [14] N.S.K. Pang. School values and teachers' feelings: A LISREL model, *Journal of Educational Administration*, 34, 64-83, 1996.
- [15] Y. Reisinger and L. Turner. Structural equation modeling with LISREL: Application in tourism, *Tourism Management*, 20, 71-88, 1999.
- [16] Y. Rezgui and A. Marks. Information security awareness in higher education: An exploratory study, *Computers & Security*, (27), 241-253, 2008.
- [17] E.E. Rigdon. Structural Equation Modeling, In G.A. Marcoulides (Ed.), *Modern Methods for Business Research*, Lawrence Erlbaum, 251-294, 1998.
- [18] K. Schermelleh-Engel, H. Moosbrugger and H. Müller. Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures, *Methods of psychological research online*, 8(2), 23-74, 2003.
- [19] E.E. Schultz, R.W. Proctor, M-C. Lien and G. Salvendy. Usability and security an appraisal of usability issues in information security methods, *Comput Secur.*, 20(7), 620-634, 2001.
- [20] M.T. Siponen. A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, 8(1), 31-41, 2000.
- [21] J.M. Stanton, P.R. Mastrangelo, K.R. Stam and J. Jolton. Behavioral information security: two end user survey studies of motivation and security practices, In: *Proceedings of the Tenth American Conference on Information Systems*, New York: 2004.
- [22] M. Tekerek. Information Security Manegement, *KSU Journal of Science and Engineering*, 11(1), 132-137, 2008.
- [23] B.D. Voss. The ultimate defense of depth: security awareness in your company, SANS Institute, white paper, 2001.
- [24] V. Yilmaz. Consumer behavior of shopping center choice, *Social Behavior and Personality*, 32, 783-790, 2004.
- [25] J. Zhang, B.J. Reithel and H. Li. Impact of perceived technical protection on security behaviors, *Inf Manag Comput Secur*,17(4), 330-340, 2009.