

# Employees' Attitude as the Determinant of Their Information Security Performance in Information Network Security Agency

Anemut Mehari Berhanu

Lecturer, Department of Psychology, Institute of Education and Behavioral Science, Dilla University

## Abstract

This study was aimed to assess the relationship between employees' attitude and information security (InfoSec) performance in the Ethiopian, INSA context. Employees' attitude was treated as the independent variable and the InfoSec performance was treated as a dependent variable of the study. Correlational research design was employed. Using a stratified random sampling technique 320 participants were sampled. AIS and ISP scales were used to collect the data. Based on the suitability of the data and research questions, percent, frequency, independent t-test, one-way ANOVA, Pearson Correlation, and regression data analysis methods were performed. Accordingly, the present study revealed the following findings. First, employees' InfoSec performance significantly differed by their sex and educational levels. Second, attitude significantly related to and predicted the employees' InfoSec performance. Based on the findings of the study some recommendations are forwarded for different stakeholders.

**Keywords:** Attitude, InfoSec Performance, confidentiality, integrity, availability

**DOI:** 10.7176/CEIS/13-2-04

**Publication date:** March 31<sup>st</sup> 2022

## 1. Introduction

Information security (InfoSec) performance is the user's ability to protect the confidentiality, integrity, and availability (CIA) of information when sending, receiving, and storing it either physically or electronically. Information security (InfoSec) problems are becoming the most prevalent issues in most organizations of this era. Both technical, individual, and psychological factors are accountable for the problem. InfoSec threats are higher in critical organizations such as military, intelligence, financial, and land management offices. Such organizations are the gallery of national level information, including the physical, economic, political, social, geographical/territorial affairs of the country. Based on the criticality of the information exposed to unauthorized users, nations, organizations, or individual users may experience serious social, economic, cultural, and political problems, or even they may fail, disrupt, and lose their existence (Salgovicova, and Prajova, 2012; Anderson, 2001).

InfoSec is a most valuable asset for the success of the individual users as well as the whole organization (Alavi, 2016; Reza, 2016). Regarding this, Ahlan et al. (2015) suggested that any organizational files are operated by their employees. When sending, receiving, storing, and using it, the CIA of the information will have a great chance to be threatened by the human factors. Information reaches in to unauthorized users and manipulates the targets.

Research progresses have been shown towards associating the psychological constructs with users' InfoSec performance. However, they are limited in the InfoSec research realm fields (Abroshan et al., 2021), other country contexts, and confidentiality dimension of InfoSec triads. However, this day, some researches have empirically examined the influence of attitude on InfoSec threats (e.g., email phishing and privacy) (Harrison, Svetieva, Vishwanath, 2016).

## 2. Statement of the Problem

As we live in the era of information, we share bulky amount of personal and organizational information. These practices lead to an increasing number of InfoSec vulnerability problems. However, the rate of vulnerability varies from person to person or organization to organization (Alavi, 2016; Hone, 2002). Malicious users of the information are grown in frequency and verity. With the introduction of newer and newer InfoSec performance improvement policies, information frauds are becoming pervasive from time to time. A Computer Security Institute reported that InfoSec incident problems grew from 46% to 49% in 2007 and 2012 respectively.

Previously, many organizational managers and manageresses were partially justify the problems and highly focus on technical competencies such as InfoSec knowledge and skills. Remarkable budgets were allocated to manage these things. But this day, some newer perspectives are emerging and special focus is given. For instance, an assessment by Safari and Azizallah (2014) and Metalidou et al. (2014) suggested that  $\geq 90\%$  of InfoSec problems in an organization are associated with human factors.

Contradicted findings in across literature have been shown. For instance, attitude towards information confidentiality, integrity, and availability are little researched except in the confidentiality dimension, and little emphasized even by most InfoSec focused organizations and most attitude studies have lacked

comprehensiveness. For example, Adeleke, Adekanye, Adefemi, Onawola, Okuku, Sheshi, James, Francis, Elegbe, Ayeni, and Tume (2011) examined the link between attitude towards InfoSec and their information confidentiality dimension, found a weak positive relationship and strong positive relationship respectively. Shown the studies conducted only from an organizational InfoSec policy compliance perspective, rather than assessing it from the general attitude model towards InfoSec issues. In addition, the users InfoSec performance variability as a function of their sex and educational levels are not examined well.

Generally, this study differs from other studies conducted previously in its objectives, area of the study, population, and samples participated, variables included, and instruments used to measure the stated variables. Therefore, considering the gaps mentioned earlier, the researcher has designed the following research questions.

1. Does the InfoSec performance of employees differ based on their sex and level of education?
2. Does attitude significantly relate to and predict the InfoSec performance of employees?

### 3. Framework of the Study

This study was generally guided by adapting attitude from the Knowledge, Attitude, and Behavior (KAB) model of Kruger and Kearney (2006), which explains the impact of positive attitude in guiding users' behavior towards the betterment of organizational InfoSec practices. However, the model has been criticized for its small positive relationship between attitude and InfoSec aspects. But the problem is not with the model itself, rather the way it applied, the conceptualization of the variables that a particular study is examining, and the way they are measured are important issues that need to be considered (Adeleke et al., 2011; Kaur and Mustafa (2013); Yazdanmehr and Wang, 2016).

### 4. Methods

A correlational research design was employed to assess the variables under study. This significantly examine the association between two or more variables and helps to make significant prediction between the variables under study (Marczy et al., 2005).

This study conducted on employees of Information Network Security Agency (INSA). The agency established in Proclamation No 130/2006 to safeguard the country from any InfoSec attacks and working to maintain an optimum InfoSec performance of national organizations and users (Federal Negarit Newspaper, 20<sup>th</sup> year, No.6, 2014). Currently, 705 males and 362 females (total of 1,067 employees) are functioning in different directorates of the agency. Generally, junior employees, supervisors, team leaders, and directors were the actual participants of the study.

The heterogeneity of the participants was captured using stratified random sampling technique. The technique also helps to make a generalization to the study population. The Yemane's (1967) sample size determination formula was used to determine and sampled 291 participants from the 5 major strata. The formula presented as:

$$n(\text{sample size}) = \frac{N(\text{population size})}{1 + N(\text{esampling error})^2}$$

Ten percent of participants were added for non-response items and non-returnable questionnaires.

The data enumerators selected the samples using a simple random sampling technique. Five enumerators were randomly assigned to each major stratum. Oral orientation given and the questionnaires administered randomly to those who are willing to participate in the study.

#### 4.1. Data Collection Instruments

*The Attitude towards the InfoSec Scale (AISS)* adapted from Ahlan et al. (2015) and Howard, (2018). attitude towards InfoSec measure. This scale is appropriate in organization setting, and has high ( $\geq .86$ ) Cronbach alpha value across organizations. It has 15 items rated on a 4-point Likert scale ranging from 1 (strongly disagree) to 4 (strongly agree). The total raw score for the scale yielded from 15 to 60. The higher the score indicated a favorable attitude towards InfoSec and the lower the score indicated an unfavorable attitude towards InfoSec.

*The InfoSec Performance Scale (ISPS)* adapted from the Bernik and Prislán(2016) employees InfoSec performance measures. The items consider the International Organization for Standardization (ISO) 31000 (2018) for users and organizations InfoSec specifications and the 10 by 10 metrics of InfoSec performance measure which helps to measure an optimum level of both physical as well as electronic InfoSec performance of the users. It has also high reliability in the previous studies. The comprises 18 Likert-type items rated on a 4-point scale ranging from 1 (*strongly disagree*) to 4 (*strongly agree*). The total raw score of the 18 items yielded from 18 to 72, in which the higher scores indicated the higher perceived InfoSec performance and the lower scores indicated lower perceived InfoSec performance of employees.

##### 4.1.1. Validation Procedure

Assuming expertise, qualification, and experience, 10 subject matter experts (SMEs) were purposively identified

and established the content validity for the total of 63 items. A draft of data collection instrument was given to the 10 panelists with clear instructions and rated each items adequacy, appropriateness, and clarity using the Lewashe's (1975) statistical content validity estimation ratio (CVR) calculation. The computational formula presented as:

$$CVR = \frac{ne - \frac{N}{2}}{\frac{N}{2}}$$

Where, *ne* - the number of panelists pointing the item 'essential' and *N*- the total number of panelists

The CVR is a technique to reject non-essential items from the initial item pools using content validity index. The value of CVR ranges from -1 to +1. The positive value indicates the appropriateness clarity of the item. The negative value indicates the ambiguity of the item, suggests the item should be modified. The value of .00 indicates that 50% of the panelists in the *N* size believes the item is essential thereby valid.

Generally, panelists rated each item using a three-point scale (*1 = not essential, 2 = useful, but not essential, and 3 = essential*). As Lewashe suggests 'essential' items best represent good content validity. If  $\geq 50\%$  of panelists perceive the item as essential and the value of CVI is closer to .99, then the overall content validity is higher. Moreover, table 1 below illustrates the established decision rule based on one-tailed test, .05 significance level, value of CVR with varying panel sizes.

Table 1: Lawshe's minimum CVR values for a varying number of panelists

Number of Panelists	Minimum acceptable CVR value
5-7	.99
8	.85
9	.78
10	.62

Finally, the response items collected from panelists, counted the number indicated as 'essential' for each item, and computed a CVR of each item using the formula. As a result, all items were retained and pass in to piloting because of recording CVR of  $\geq .62$ .

#### 4.1.2. Translation Procedure

All data collection instruments were translated from source language (English) to target language Amharic in which the official working language of the participants by the SMEs. The practice helps to improve the contextual validity and reliability of the instrument, data, and/or finding Valmi and Wilaiporn (2011). It also helps to determine the appropriateness, relevance, and adequacy of wording of items; brings high response quality; and makes participants feel comfortable (Zelt et al., 2018)

A total of three SMEs assumed to be enough for masters thesis and purposively recruited and made translations. One expert has made the forward translation and the other one expert has made the backward translation. Both of them were fluent in Amharic language and were English language literature lecturers. Finally, the remaining one expert (*a dual degree holder in psychology and in information system security*) has edited, ensured the equivalence of the two versions of the instrument and approved it for a pilot data collection. All issues related to the clarity, validity, and professionally of terms or wording of items, and its suitability to the context of participants were significantly assessed.

#### 4.1.3. Pilot Testing

Pilot testing conducted on randomly selected 50 (17 female and 33 male) employees. These participants were purposively excluded from the main study. The size of the sample determined based on most quantitative study suggestions in which  $\geq 30$  participants are sufficient for establishing good instrument reliability and response rate in quantitative researches (1) and my research advisor (Dr. Dame) of 50 to 70 participants for piloting (2).

The reliability index of the tool computed using Cronbach Alpha ( $\alpha$ ) value. It best indicates the internal consistency of items with Likert-type scales. As a rule of thumb  $\alpha \geq .9$ ,  $.8 \leq \alpha \leq .89$ ,  $.7 \leq \alpha \leq .79$ ,  $.6 \leq \alpha \leq .69$ ,  $.5 \leq \alpha \leq .59$ , and  $\alpha \leq .5$  interpreted as excellent, good, acceptable, questionable, poor, and unacceptable respectively. However, in most cases,  $\alpha \geq .70$  considered as a good indicator of scale reliability (Schattner and Mazza, 2015). See the Cronbach  $\alpha$  index computed for pilot study in table 2 below.

To be a scale reliable, all items must be positively correlated with the item total score within it. Deleting items with weak and negative item-total correlation significantly increase the  $\alpha$  coefficient of the scale (Teijlingen and Hundley (2014). Accordingly, one item from the ISPS was deleted for its context negative item-total correlation output (-.062). Removing it brings a significant advantage in increasing the value of  $\alpha$  coefficient and improving the reliability of remaining items in measuring the study variables. As a result, except for an item deleted, the item-total correlation of all the remaining items was .77, indicates high item-total correlation value. Generally, based on the results of the pilot study, some necessary modifications have been

made and the actual data collection was performed.

Table 2: Statistical outputs of  $\alpha$  output for the original measure, pilot study, and main study

Scales & sub-scales	No of items	Original Measure	Pilot study	Main study
AISS	15	.86	.83	.89
ISPS	18	On ave., .79 - .86	.89	.94

Source: SPSS output

#### 4.2. Data Collection Procedure

Five data enumerators (one per major stratum) were purposively recruited and familiarized with the data collection instruments. Considering their experience, knowledge, and exposure to the data collection practices, 1:30 hours of training on how to approach participants, describe the purpose of the study, take their consents, administer, and collect the response questionnaires. The questionnaires were administered by hands before the participants started their regular tasks in their office.

#### 4.3. Data Analysis

Data handled by Statistical Package for the Social Science (SPSS V. 25). Assuming the appropriateness of the data nature and suitability of research questions frequency, percentage, independent sample t-test, one-way ANOVA, Pearson Correlation Coefficient Matrix, and regression data analysis techniques were employed. In addition, considering unequal sample sizes between groups, the Scheffe post hoc ANOVA test was employed.

#### 4.4. Data Screening and Test of Model Assumptions

The correctness of data entry, absence of missing and extreme values, and normality of the data were examined using frequency counting and extreme score elimination techniques. Generally, out of 320 distributed questionnaires 296 were qualified for the analysis.

The assumption of independence (the scores independence of each other), normality (the normal distribution of the test scores or dependent variable within two populations, linearity, and homogeneity of variance (the equality of variance in the test variable in the two populations) were tested and satisfied. Generally, the statistical significance level of the study was set at alpha .05.

### 5. Results

#### 5.1. Employees Demographic Characteristics

Table 3: Participants demographic characteristics

Variable	Label	Figure	Percent
Sex	Female	101	34.12 %
	Male	195	65.88 %
Level of education	Diploma	26	8.78 %
	First degree	218	73.65 %
	Second degree	52	17.57 %
	<b>Total N</b>	<b>296</b>	<b>100 %</b>

Table 3 above shows the demographic data of participants who are qualified for data analysis. This implies that reasonably representative participants were sampled for drawing inferences about the target population using the sample data.

#### 5.2. Differences in InfoSec Performance by the Sex of Employees

Table 4: Independent t-test analysis

Dependent Variable	Sex	N	Mean	SD	t	P
InfoSec Performance	Female	101	37.45	5.64	17.42	.000
	Male	195	52.17	7.47		

Employing the independent sample t-test, the InfoSec performance of employees significantly differed by their sex [ $t(1, 294) = 17.42, p = .00, \text{Cohen's } d = 2.21$ ]. This revealed that compared to females ( $M = 37.45$ ), males ( $M = 52.17$ ) have better performance in keeping the computer and physical information confidentiality, integrity, and availability. The effect size also shows male employees scored 2.21 standard deviation higher on the InfoSec performance scale than females. Besides, the Levene test result illustrates [ $F(1, 294) = 27.5, p = .88$ ], indicates the variances in male and female participants were not significantly different or variances in both sexes were approximately equal.



### 5.3. Employees InfoSec Performance Differences by their Level of Education

Table 5: A one-way ANOVA analysis (N= 296)

Dependent Variable	Educational Levels	N	Mean	SD	Df		F	P
					B/n groups	W/in Groups		
InfoSecPerformance	Diploma	26	26.73	2.93	2	293	217.71	.00
	1 <sup>st</sup> degree	218	41.04	5.71				
	2 <sup>nd</sup> degree	52	56.42	4.34				

One-way ANOVA was employed to examine the employees' InfoSec performance difference as a function their level of education. The result revealed that the employees' InfoSec performance significantly differed by their level of education [ $F(2, 293) = 217.71, P < .05, \eta^2 = .60$ ]. The Scheffe post-hoc ANOVA result further shows the presence of significant mean score difference between: [*diploma and first degree; diploma and second degree; first degree and second-degree educational levels*]. The mean shows  $M = 56.42, M = 41.04,$  and  $M = 26.73$  for second degree, first degree, and diploma holders respectively.

Generally, the analysis illustrated that employees with higher level of education tend to have better performance to protect the confidentiality, integrity, and availability of information than those of employees with lower level of education.

### 5.4. The Relationship between the Predictor and Criterion Variables

Table 6: Pearson correlations analysis (N=296)

Variables	Attitude	ISP
Attitude	1	
ISP	.59**	1

\*\* Correlation is significant at the 0.01 level (1-tailed)

Pearson Correlation Coefficient was performed to assess the relationship among the study variables. Accordingly, the result indicates the InfoSec performance scores of employees positively related with attitude scores ( $r(294) = .59, p < .01, r^2 = .352$ ). This implies being growing in favorable attitude tend to pay more attention to protect the agency's information from the illegitimate and malicious users. Moreover, the magnitude of the correlation coefficient ( $r = .59$ ) implies a moderate relationship between employees' attitude and their InfoSec performance in the INSA context.

### 5.5. Predicting the InfoSec Performance of Employees' using the Predictor Variables

Table 7: Regression analysis (N = 296)

Model	Variables entered	Adjusted R <sup>2</sup>	t	F	P
1	Attitude	.568	2.89	65.61	.004

Source: Questionnaire data

To predict the InfoSec performance of employees using the predictor variable, the regression analysis was employed. Therefore, attitude significantly predicts the employees InfoSec performance scores ( $R^2 = .568, F(1, 294) = 65.611, P = .004$ ). Hence, 56.8 % of the variance in the InfoSec performance scores of employees is explained by their attitude towards InfoSec. Meaning, 56.8 % of the variance in the employees' InfoSec performance scores accounted for by a unit of change in the employees' attitude scores. However, the remaining 43.2 % of the variance in the employees InfoSec performance explained by the unknown factors which are not considered in the present study.

## 6. Discussion

Regarding the employees InfoSec performance difference by the sex, a statistically significant finding was obtained. Male and female employees significantly varied in their InfoSec performance scores. This means that males have shown relatively better InfoSec performance than female employees. This finding confirmed the works of Abroshan et al. (2021) and Fatokun, Hamid, Norman, and Fatokun (2019) in those women are more responsive to phishing emails than males. This behavior brings more susceptibility of information beaches which indicates a weak InfoSec performance. However, their study limited to electronic and online based InfoSec bases. Focus on the level of education, the present study reveals employees with higher education level shown higher level of InfoSec performance in the electronic and physical form and CIA dimensions. Similarly, in Metalidou et al. (2014) identified employees with higher levels of educational status are less vulnerable to InfoSec problems. More education connected with the development of pragmatic skills, knowledge, awareness, and practices which ensures the user to keep the information with better organization, integration, and confidentially. Consciousness of information beaches also grown and try to make the files private, inaccessible to the authorized, and address it to intended users (Malahat, 2013).

The present study also indicated a positive and moderate relationship between employees' attitude and their InfoSec performance. Kaur and Mustafa (2013) found a positive relationship between the attitude and loss of information privacy ( $r = .002$ ,  $r = .71$ , and  $r = .23$ ) respectively. However, all were based on a single (confidentiality) dimension of InfoSec triads, lacks inclusiveness of CIA InfoSec measures. Finally, the regression analysis of the present study implies 56.8 % of variance in the employees InfoSec performance scores by their InfoSec attitudes. This finding supported by the works of Nasir, Arshah, Ab, Mohd (2017); Kim, and Kim, (2022) and Michel, Dirk, Etienne, Ronald, Ciska, Yvan, (2011). According to them strong compliance towards organizational InfoSec standards, policies, and cultures showed as the positive predictors of low susceptible to information vulnerability problems. But the study doesn't directly examine the employees' attitude and only depend on a single InfoSec perspective.

## 7. Conclusion

Based on the findings the study, the following conclusions are made. First, the employees InfoSec performance significantly differed as a function of their sex and level of education. This implied that employees with more education tend to acquire more pragmatic experiences, awareness, and responsibilities to protect information from unauthorized deletion, modification, and use. They require logging controls for all folders and computer, use antiviruses and physical access controls of any information, and never share passwords and shelf keys without having a complete responsibility of the user.

Second, attitude positively related to and predicted the InfoSec performance of employees in the Ethiopian, INSA context. This implied that employees with favourable attitude towards information confidentiality, integrity, and availability tends to develop a strong feeling of responsibility to protect the information from illegitimate users both in printed and electronic forms. Periodically maintain the database and place of documents in their computer or file shelves to keep the security of their agency information.

## 8. Recommendation

- Candidates with positive attitude on InfoSec issues found to be the primary choice of hiring organizations and employers particularly for InfoSec related job vacancies.

## 9. Limitation of the Study

- Due to the lack of recorded data about the employee's day to day InfoSec performance, this study was conducted based on the basis of participants personal views towards their InfoSec performance

**Note:** *this article has no any conflict of interest and funding issues*

## References

- Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). *Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process*. *IEEE Access*, 9, 44928–44949. doi:10.1109/access.2021.3066383
- Adeleke I. T., Adekanye A. O., Adefemi S. A., Onawola K. A., Okuku A. G., Sheshi E. U. James-Adeniran J. A., Francis M., Elegbe T. R.O., Ayeni A. M. and Tume A. A. (2011). Knowledge, Attitudes and Practice of Confidentiality of Patients' Health Records among Health Care Professionals at Federal Medical Centre. *Nigerian Journal of Medicine*, Vol. 20 No. 2, ISSN 1115 – 2613
- Harrison, B., Svetieva, E., and Vishwanath, A., (2016). *Individual processing of phishing emails*. *Online Information Review*, 40(2), 265–281. doi:10.1108/OIR-04-2015-0106
- Ahlan, A., R., Lubis, M., Lubis, A., R. (2015). *Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures*. *Procedia Computer Science*, 72(), 361–373. doi: 10.1016/j.procs.12.151
- Alavi, R. (2016). *A Risk-Driven Investment Model for Analysing Human Factors in Information Security*. Doctoral Thesis, University of East London
- Alavi, R., Islam, S., Mouratidis, H., (2016). An information security risk-driven investment model for analyzing human factors. *Journal of Information and Computer Security*, vol. 24,(2)
- Anderson, R. (2001). *Soc Seventeenth Annual Computer Security Applications Conference - New Orleans, LA, USA (10-14 Dec. 2001)] Seventeenth Annual Computer Security Applications Conference - Why information security is hard - an economic perspective*, 358–365. doi:10.1109/ACSAC.2001.991552
- Bernik, I., & Prislán, K. (2016). *Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation*. *PLOS ONE*, 11(9), Doi: 10.1371/journal.pone.0163050
- Computer Security Institute (CSI), (2007 & 2012). *Computer security and crime survey*. Greenwich
- Fatokun, F. B., Hamid, S., Norman, A., and Fatokun J. O. (2019). The Impact of Age, Gender, and educational level on the Cybersecurity Behaviors of Tertiary Institution Students: *An Empirical investigation on Malaysian Universities*. *Journal of Physics: Conference Series*, Volume 1339, International Conference

- Computer Science and Engineering (IC2SE) 26–27 April 2019, Padang, Indonesia.  
<https://iopscience.iop.org/article/10.1088/1742-6596/1339/1/012098/meta>
- Nasir, A., Arshah, R. A., Ab, H., Mohd, R. (2017). *International Conference on Information System and Data Mining - ICISDM '17 - Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture*, 56–60. doi:10.1145/3077584.3077593
- Hadlington, L., Popovac, M., Janicke, H. Y, Iryna, J., Kevin (2018). *Exploring the role of work identity and work locus of control in information security awareness*. *Computers & Security*, (), S0167404818308897. Doi:10.1016/j.cose.2018.10.006
- Hadlington, Lee; Chivers, Sally (2018). *Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors*. *Policing: A Journal of Policy and Practice*, (), -. doi:10.1093/police/pay027
- Hone K., Eloff, J.H.P., (2002). *Information security policy — what do international information security standards? 21(5)*, 402–409. doi:10.1016/s0167-4048(02)00504-7
- Howard, D. J., (2018). Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents. Graduate Theses and Dissertations.
- Kaur, J., Mustafa, N. (2013). *[IEEE 2013 International Conference on Research and Innovation in Information Systems (ICRIIS) - Kuala Lumpur, Malaysia (2013.11.27-2013.11.28)] 2013 International Conference on Research and Innovation in Information Systems (ICRIIS) - Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME*. doi:10.1109/icriis.2013.6716723
- Kim, H. E., Kim, J. H. (2022). A Survey on the Attitude of Social Groups toward Security, Privacy, and Confidentiality of Health Information: An Original Paper Authors and Affiliations. *Journal of Korean Society of Medical Informatics* 1999; 5(3): 63-76. DOI: <https://doi.org/10.4258/jksmi.1999.5.3.63>
- Kruger, H. A., and Kearney, W. D. (2006). A prototype for assessing information security awareness. *Journal of computers & security* (25) 289–296. DOI: 10.1016/j.cose.2006.02.008
- Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology*, 28 (4), 563-575.
- Malahat, P. (2013). Information Security Vulnerability in an Iranian Context from Human Perspective (Electrical Industry). A Dissertation Submitted in Partial Fulfillment of The Requirements for The Award Of The Degree Of Master Of Science (IT Management)
- Marczy, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of research design and methodology*. New York
- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., ann Skourlas, C., (2014). Human factor and information security in higher education. *Journal of Systems and Information Technology*, 16(3), 210–221. doi:10.1108/jsit-01-2014-0007
- Metalidou, Efthymia; Marinagi, Catherine; Trivellas, Panagiotis; Eberhagen, Niclas; Skourlas, Christos; Giannakopoulos, Georgios (2014). *The Human Factor of Information Security: Unintentional Damage Perspective*. *Procedia - Social and Behavioral Sciences*, 147(), 424–428. Doi: 10.1016/j.sbspro.2014.07.133
- Michel, D., Dirk, D., Etienne, D. G., Ronald, B., Ciska, C., Yvan, V., (2011). *Informative privacy and confidentiality for adolescents: the attitude of the Flemish pediatrician in 2010.*, 170(9), 1159–1163. doi:10.1007/s00431-011-1427-4
- Prislan, K., Mihelia, A., Bernik, I. J. (2020). *A real-world information security performance assessment using a multidimensional socio-technical approach*. *PLOS ONE*, 15(9), e0238739–. doi:10.1371/journal.pone.0238739
- Reza, M., A. (2016). A Risk-Driven Investment Model for Analysing Human Factors in Information Security. PhD Thesis University of East London Architecture, Computing and Engineering <https://doi.org/10.15123/PUB.5379>
- Safari, L., and Azizallah, R., (2014). "The role of human factors in information system security." *Advances in Environmental Biology*, . Gale Academic OneFile, [link.gale.com/apps/doc/A385069540/AONE?u=anon~6fcc4b59&sid=googleScholar&xid=dc088ba1](http://link.gale.com/apps/doc/A385069540/AONE?u=anon~6fcc4b59&sid=googleScholar&xid=dc088ba1). Accessed 25 Feb. 2022.
- Salgovicova, J. and Prajova, V. (2012). Faculty of Materials Science and Technology in Trnava Slovak University of Technology in Bratislava. Doi: 10.2478/v10186-012-0019-0, Volume 20
- Schattner P, and Mazza D., (2015). Importance of doing a pilot study. *Journal of Malaysian Family Physician*, 5 (8), 70-73
- Teijlingen R. and Hundley V., (2014). Why a pilot study? *Journal of Psychology*. DOI: 10.1823/206198.
- Valmi D. S., and Wilaiporn, Rojjanasrirat (2011). *Translation, adaptation and validation of instruments or scales for use in cross-cultural health care research: a clear and user-friendly guideline*. , 17(2), 268–274. doi:10.1111/j.1365-2753.2010.01434.x
- Yazdanmehr, A., and Wang, J., (2016). *Employees' information security policy compliance: A norm activation perspective*. *Decision Support Systems*. doi:10.1016/j.dss.2016.09.009

---

Zelt S, Recker J, Schmiedel T, vom Brocke J (2018) Development and validation of an instrument to measure and manage organizational process variety. PLoS ONE 13(10): e0206198. <https://doi.org/10.1371/journal.pone.0206198>