Personality Difference Associated with the Information Security Performance of Employees' in the Information Network Security Agency (INSA)

Anemut Mehari[1] Dame Abera[2]
1.Lecturer, Department of Psychology, Institute of Education & Behavioral Science, Dilla University
2.Associate professor, School of Psychology, College of Education & Behavioral Studies, Addis Ababa University

Abstract
Now a day information security (InfoSec) is a prime focus and critical aspect of all organizations as well as individual users. The major purpose of this study was to assess the association between employees' personality difference and InfoSec performance in the Ethiopian, INSA context. Accordingly, the five-factor personality difference (OCEAN) was treated as the independent variable, while the InfoSec performance was treated as a dependent variable. Based on the quantitative approach, a correlational research design was employed. A total of 320 participants were selected using a stratified random sampling technique. The BFFI and ISP scales were administered to collect the quantitative data. The Independent t-test, one-way ANOVA, Pearson Correlation, and hierarchical multiple regression data analysis methods were performed to address the research questions. Accordingly, the present study revealed the following findings. Firstly, employees InfoSec performance significantly differed by their sex, level of education, job positions, and length of InfoSec training taken. Secondly, age, work experience, and personality difference were significantly related to the employees InfoSec performance. Thirdly, employees' personality difference significantly predicted their InfoSec performance both independently and jointly. Generally, personnel recruiters, employers, trainers, and interventionists were recommended to consider their candidates' background characteristics and personality difference when they deliver their services.

Keywords: Personality Difference; Information Security (InfoSec) Performance
DOI: 10.7176/RHSS/12-1-01
Publication date: January 31st 2022

1. Introduction

As we live in the era of information and continuous advancements of technology, we send, receive, or store bulky amount of critical organizational information such as files, documents, etc. in each day (Salgovicova and Prajova, 2012). Accordingly, the interaction with the information leads to the greater security issues. However, the rate of vulnerability varies among employees and organizations (Michael et al., 2016).

In the early time, various researchers relate information security (InfoSec) problems with the technical aspects of the users or employees such as skill, knowledge, and competencies (Henry et al., 2018). But InfoSec has quickly evolved from a purely technical discipline to a social, economic, and geopolitical strategic concept. At the 2010, twenty-eight world leaders declared that InfoSec-attacks now threaten international prosperity, security, and stability (Geers, 2011). In regard to this, Shropshire et al (2006) and Taherdoost (2016 & 2017) found lack of users InfoSec awareness as a number one obstacle to achieve the good InfoSec posture of the user as well as the organization. They also suggested continuous and periodic InfoSec awareness trainings as a solution to improve the InfoSec performance (confidentiality, integrity, and availability or CIA) of users or reduce InfoSec related threats. However, Alavi and Micah (2014) and Uffen et al (2013) argued that 'even if users' InfoSec awareness level has been grown, organizations and users cannot achieve their maximum InfoSec performances'. An awareness of information confidentiality, integrity, and availability is the vigilance of understanding and perception of various InfoSec threats. Understanding threats alone seems insufficient to motivate employees to take actual actions in preventing InfoSec problems. Because InfoSec is not a single matter of Information Technology, rather it's beyond the technical aspect of InfoSec awareness in that it incorporates the various psychological constructs (e.g., security-sensitive personality types) of the users.

Therefore, information CIA has become a critical issue, most valuable asset (like every physical asset that must be protected), and a critical success factor for any and the whole organization and individual customers (Tenney et al., 2015). Regarding this, Albladi and Weir (2017) implied that many organizational data are pervasively dependent on and operated by their employees. The CIA of these data have a great chance to be threatened by the human factors (user's individual and psychological characteristics). The data vulnerability may happen in either of sending, receiving, storing, or using it. Similarly, Herath and Rao (2009) indicated several personal, organizational, national, or international level information have been reached to unauthorized users either deliberately or non-deliberately and used for manipulating the targets. In all those information insecurity experiences, humans with their various factors played significant roles. Employee's interaction with any information in their hands or devices; use of strong passwords for computers, folders, as well as documents; use of backups for electronic and non-electronic files, is highly dependent on and/or varied across their personality differences or types. The employees' ability in protecting the information confidentiality from unauthorized access, integrity from the unauthorized information modification, and availability to the authorized users particularly when transacting it both physically or electronically is significantly differed by their personality differences. Also, the employees use of use of trusted and/or internal data management system; password protected computers and/or locked shelfs is influenced by their security conscious personality characteristics.

In most cases, InfoSec researchers have anticipated the relationship between personality type and user's InfoSec attacks (e.g., social engineering-based attacks); And progresses have been shown towards correlating psychological variables with the critical aptitudes that users must possess for successful InfoSec performance and utilize it for InfoSec candidate selection purposes. But mostly they were limited in the InfoSec research realm fields (Nelson & Yorke, 2015), other countries contexts, and only confidentiality dimension of InfoSec triads (Alhassana & Adjei-Quayeb, 2017). However, in this day, some research has empirically examined the influence of personality difference on InfoSec threats (e.g. email phishing response and loss of one's information confidentiality). But, beyond conducting little studies in the area, most researches are not conducted based on the compressive measure of InfoSec or CIA triads. Literature survey has shown most researchers extensively examined only the confidentiality dimension. The two important dimensions of information such as integrity and availability remain under touched in most researches. In addition, contradicting findings across researchers, time, place, settings or contexts is also another additional gap in the area. For instance, Jain and Pal (2017) indicated neuroticism as the only personality type which negatively correlated with phishing email responses resulted in information loss. In contrast, Pouransafar et al. (2015) found openness, extraversion, and agreeableness significantly increased the user's tendency to comply with phishing email requests and engage them to high-level information confidentiality loses. McCrae (2017) found fewer workplace information confidentiality accidents with employees of conscientious personality and higher rate of information deletion with employees of openness, extraversion, agreeableness, and neuroticism types.

Generally, different researchers studied the issue for their own objectives or interests. However, considering the gaps assessed earlier and the need to fill them, the present study attempted to test the issue under Ethiopian, INSA context. It empirically examined the compressive InfoSec performance (CIA) of employees associated with personality difference. It's also further compressive by assessing both physical (e.g., printed documents) and electronic (e.g., in the computer system) InfoSec performances.

1.2. Statement of the Problem

For many years, most organizational managers attributed their employees' InfoSec performance problems to poor technical competencies like awareness, knowledge, and skills deficiencies and poor budget allocated for InfoSec (Lapsley and Hill (2009), Metalidoua et. al., (2014), and Parson et. al. (2010). As a result, hiring competent InfoSec experts, delivering continuous InfoSec awareness, skill, and knowledge development trainings were taken as a priority role of the managers so as to bring an optimum InfoSec performance of their employees and organizations (Wendy and Gunawan, 2019). However, InfoSec problems far from resolved. Competent InfoSec experts and continuous InfoSec trainings do not fully ensure the InfoSec performance of organizations and its employees'. Computer Security Institute survey in Europe and America indicates the pervasive and complex nature of InfoSec problems from time to time. For instance, in 2007, 46% of the 487 participants exposed to at least one InfoSec incident problem in a given 12 months. While in 2012, 49 % of 512 employees were exposed to an average of two information confidentiality losses in a single year. By 2013, almost 19 private or governmental, civic or profit, economic, social, or political organizations have been stopped their regular functions, become stagnant, totally failed, or replaced by other new forms in every 2 or 3 years. Besides, a study by Jain and Pal (2017) indicated nearly 56 % of users in the organization lost their electronic information confidentiality by unauthorized users.

Ethiopia is not also a different nation. InfoSec problem incidents are still very prevalent and shows an exponential annual increase. For example, the Ethiopian Management Institute database system has been lost. Approximately 3 months were taken to re-feed the fragmented data into the system (Risk Assessment Committee Report, 2016). Generally, the problem was attributed to the user's improper management of the system and information in it. They were not too much concerned about being targeted for information theft. Similarly, the INSA's InfoSec Risk Assessment Team in 2019 reported a twice more InfoSec incidents than the 2015. Nine out of ten incidents were roughly attributed to employees' weak link to InfoSec issues and awareness. Due to employees' involvement, a 9 % increase of InfoSec threats has been reported from 2017 to 2019. As we are becoming through building a strong attachment to information (more on electronic forms), our security defects will also significantly grow in the future. Overall, these implies a pervasive increment of InfoSec problems. Technical skills, knowledge, and awareness have been over emphasized, while the psychological constructs like individual and personality differences looks undermined.

Organization without its people users is like a vacuum. Employees are the heart of any organization either for success or failure. Problems in it arises from those actors. Accordingly, Karwowski and Glaspie in 2018 found that > 90% of organizational InfoSec problems are caused by human factors rather than technical problems. InfoSec performance improvement standards and policies function better when users are highly risk perceptive and security conscious in their personalities. However, in most cases, little attention and budget has been allocated to the issue in comparison to technical skill development practices. Generally, the following research questions were designed and answered.

1. Does the InfoSec performance of employees vary as a function of their sex, level of education, job position, and length of InfoSec training taken?
2. Do age, work experience, and personality difference significantly relate to the InfoSec performance of employees?
3. Do age, work experience, and personality difference significantly predict the InfoSec performance of employees?

1.3. Framework of the Study

The Big-Five Factor Personality Model of John & Srivastava (1999) was employed to guide the study. This model, explains the employees' InfoSec performance using the five personality types usually called OCEAN. Openness (being curious to actions, things, and ideas), Conscientiousness (being organized), Extraversion (being outgoing and sociable), Agreeableness (being cooperative and helpful with others), and Neuroticism (emotionally unstable). According to Shropshire et al. (2006), big-5 is the leading theoretical model used to measure and predict InfoSec performance using the 5 factors in a diverse and complex environment. In addition, Bansal (2011), Campbell et al (2010), and Uffen et al (2013) confirms it as a good model for understanding personality difference associated with InfoSec issues particularly in organization contexts.

2. Methods

Based on quantitative approach, a correlational research design was employed. As Marczy et al. (2005) indicated correlational research design is used to test the statistical association between two or more variables (e.g., employees' personality differences and InfoSec performance) and helps to make significant prediction between the variables under studied.

All 1,067 staffs (705 male & 362 female) of Information Network Security Agency (INSA), employees were the target population of the study. However, janitors, child day care, and gate security staffs were purposively excluded due to their work nature and inconsistent availability during data collection time. Therefore, junior employees/experts, supervisors, team leaders, and directors of the agency were the actual participants of the study. They have an adequate exposure and long-lived in InfoSec issues such as experience sharing practices, cultures, and trainings in particular to organizational contexts. As a result, these will significantly matter the validity and quality of the data as well as the study.

A stratified random sampling technique was employed to capture the diversity of the participants in terms of directorates they work on, sex, job position, etc. As suggested by Alvi (2016) and Taherdoost (2016), it also gives a confidence to make a generalizable conclusion to the study population. With its advantage in providing relatively accurate sample size (Ajay and Micah, 2014), the Yemane's (1967) simplified sample size determination formula with 95% of confidence interval and 5% acceptable sampling error was used to determine 291 participants from the 5 existed strata (Aerospace, Engineering solution, Cyber security, Assurance, and Human resource). The formula presented as: $n = \frac{N}{1+N(e)^2}$; Where, n represented sample size, N represented population size, and e represented sampling error (level of precision).

Generally, assuming the non-response items and non-returnable questionnaires, 10 % of participants were added, as suggested by Taherdoost (2017). Therefore, a total of 320 participants were selected for this study. Even though, proportional sampling formula employed to determine the proportional sample size with respect to population size in each stratum, the samples were generally disproportional across strata. Because the samples taken from each stratum were significantly varied.

Following the sample size determination in each stratum, the data enumerators with the guidance of the researcher selected the actual research participants using a simple random method. Before one day of the data collection day, the 5 research assistants were randomly assigned to each five major strata and sent to each stratum office. They provided oral orientation about the aim of the study to the whole staff in their office and randomly administered the questionnaires to those who were consented to fill the questionnaire. The same practice was done by the data enumerators in each data collection stratum.

2.1. Measures

The participants' demographic data were collected using 6 questions such as sex, age, work experience, level of education, job position, and length of InfoSec training taken. *The Big Five-Factor Personality Inventory (BFFPI)* was adapted from the John and Srivastava (1999) and used to measure employees' personality difference. BFFI has wide applicability in measuring employee's personality difference in the InfoSec areas with showing consistently high convergent validity with other self-report scales and peer rating big-five measures (John and Srivastava, 1999); inherent generalizability significance in its systematic and comprehensive approach to personality (Metalidoua et al., 2014); complete taxonomy of terms that allowed employees to describe themselves and others (Alavi, 2016); organization based behavioral patterns associated with the factors which are well known in comparison to a large number of specific factors (John and Srivastava, 1999); and with its sub-scales, on average it has a high Cronbach alpha value in various studies, across organizations, various translations, and different population (Shropshire et. al., 2006).

The BFFPI has a total of 30 items in the 5 sub-scales-OCEAN (openness, conscientiousness, extraversion, agreeableness, and neuroticism). Each item in each sub-scale was rated on a 4-point Likert scale ranging from 1 *(strongly disagree)* to 4 *(strongly agree).* To avoid possible response biases, some of the items were reversely worded. In general, each sub-scale has consisted of 6 items yielded a total raw score ranging from 6 to 24. Composite scores for each sub-scale were calculated following the reverse coding of the negatively worded items. The higher the scores in each sub-scale indicated the dominant personality type in the big-five factor personality measure.

The InfoSec Performance Scale (ISPS) was adapted from Anderson (2007) InfoSec performance measure. It comprises 18 Likert-type items. It measures the compressive InfoSec performance using the CIA triads (Uffen et. al., 2013). In addition, the ISPS developed based on the International Organization for Standardization/ISO 31000 (2018) for users and organizations InfoSec related measure specifications; the 10 by 10 metrics of InfoSec measure which helps to evaluate the optimum level of physical and electronic InfoSec performance of the users; the employees' perception towards their InfoSec performance in organization settings (Hinson, 2003). It has also a high reliability (between Cronbach alpha .79 to .86 in the previous studies (Macada, 2015).

Like BFFPI, ISPS items rated on a 4-point Likert-type scale ranging from 1 *(strongly disagree)* to 4 *(strongly agree).* Some items ISPS were reversely worded. The total raw score of the 18 items yielded from 18 to 72, in which the higher scores indicated the higher InfoSec performance, the lower scores indicated lower InfoSec performance of employees, and the score 34 to 40 shows moderate level InfoSec performance.

2.2. Validation Procedure

Based the Lawshe's (1975) .62 minimum CVR value decision rule for 10 panelists in one-tailed test and .05 significance level, a panel of 10 subject matter experts (SME's) were purposively identified *(5 from social psychology and 5 from information system security fields)* and established the content validity for the total of 63 translated questionnaire items. Their level expertise, qualification, and experience were considered. A draft copy of data collection instrument was given to the 10 panelists by hands with clear instructions on how they judge the adequacy, appropriateness, and clarity of each item and the way they rate each item. Accordingly, the Lewashe's (1975) content validity technique that involves the statistical validity estimation ratio was employed. The statistical content validity ratio (CVR) is useful to reject a specific non-essential item from the initial item pool using item statistics or content validity index (CVI - the mean of the CVR values of the retained items) for the whole item pool. The computational formula is $\mathrm{CVR} = \frac{\mathrm{ne}-\frac{\mathrm{N}}{2}}{\frac{\mathrm{N}}{2}}$; where ne - the number of panelists pointing the item *'essential'* and N- the total number of panelists.

The value of CVR ranges between -1 and +1. Positive values indicate the item is appropriate and clear; negative values indicate the item needs to be reworded, changed, or rejected; and the value of .00 indicates 50 % of the panelists in the N size believed that the item is essential thereby valid. In general, if 50% and more panelists perceive the item as essential and the value of CVI is closer to .99 then the overall content validity is higher (Lewashe, 1975, Zelt et. al., 2018). Therefore, the panelists were rated each item using a three-point scale *(1 = not essential, 2 = useful, but not essential, and 3 = essential)*. '*Essential'* items best represent good content validity.

Finally, the responses collected from the panelists, counted the number indicated as *'essential'* for each item, and computed a content validity ratio of each item using Lawshe's formula. Therefore, based on the decision rule, only items which meets the minimum CVR value (≥ .62) were accepted, while the remaining items having CVR value of <.62 were removed. Generally, two items (one from the openness sub-scale and the other one from the extraversion sub-scale) were rejected and the rest, which recorded ≥.62 retained and used for the pilot study. Besides, the content validity index (CVI) computed for all retained items in the scale was 89 %, viewed the instrument is valid and acceptable (Zelt et al., 2018).

2.3. Translation Procedure

Translating the data collection instrument from the source language to the target language significantly improves context validity, reliability and validity of the instrument, data, and the findings of the study (Raudenbush, 2015);

helps to determine the appropriateness, relevance, quality, adequacy, and wording of items; obtains high response quality, and makes the participants feel comfortable (Dhamani and Richter, 2011). Accordingly, all the scales were translated from the English to Amharic language *(the official working language of the participants)* by the SMEs. Backward translation was made to test the equivalence of items in the target and original language.

Based on Dhamani and Richter (2011) suggestion of 3-9 instrument translation experts for students' theses at the master's degree level, a total of 4 SMEs' were participated in both forward and backward translation practices. One expert was made the forward translation and the other one expert made the backward translation. Both of them were fluent in Amharic language and were English language literature lecturers. Finally, the 2 SMEs (*one social psychologist and one information system security graduate*) were came together, edited, ensured the equivalence of the two language versions of the instrument, and approved it for a pilot data collection. Moreover, the experts assessed the clarity, validity, professionality of terms or wording, and suitability of items to the context of the participants.

2.4. Pilot Testing

Beyond establishing the contextual reliability of the scales, pilot testing allows to ensure the adequacy, length, and wording of items and the instrument as a whole. In the case of quantitative study, ≥ 30 pilot participants are enough for establishing good instrument reliability and response rate (Schattner and Mazza, 2015). Therefore, the reliability and practicality of the instrument in particular to Ethiopia, INSA context was tested using the randomly selected 50 (*17 female and 33 male*) employees. The pilot participants were selected from a separate office of the agency, but represented almost similar characteristics to the main study samples *(purposively excluded in the main study).* The size of sex-based samples was determined as suggested by Taherdoost (2017). The proportional sample size was taken in relation to the total sample size of the main study participants. The formula is Using $\mathrm{Np} \times \frac{\mathrm{n}}{\mathrm{N}}$ formula; Where Np - total sample size of the study indicated female (110) or male (210); n - the total sample size of the pilot study (50); and N - total sample size of the study (320).

Assuming its relevance in showing better internal consistency of items with Likert-type scales (Teijlingen and Hundley, 2014), Cronbach Alpha (α) reliability index was computed. As a rule of thumb, the following coefficient interpretation are suggested: if α ≥ .9 is excellent, .8 ≤ α ≤ .89 is good, .7 ≤ α ≤.79 is acceptable, .6 ≤ α ≤ .69 is questionable, .5 ≤ α ≤ .59 is poor, and α ≤ .5 is unacceptable. However, in most cases, Cronbach α of ≥ .70 was considered as a good indicator of scale reliability (Zelt et. al., 2018). *See the Cronbach α index computed for pilot study in table 3 below.*

To be a scale reliable, all items need to correlate positively with the item total score. Deleting items having a weak and negative item-total correlation can significantly increase the α coefficient of the scale (Alhassana & Adjei-Quayeb, 2017). Accordingly, two items (*one item from neuroticism sub-scale and the other one item from the ISPS*) were deleted for their context irrelevancy and negative item-total correlation output *(-.057, and -.062)* respectively. Removing them brings a significant advantage in increasing the value of α coefficient and the reliability of remaining items. As a result, except for those items deleted, the item-total correlation of all the remaining items was .77, indicated high item-total correlation value as Albladi & Weir (2014) suggested. Generally, based on the results of the pilot, some necessary modifications such as language and ambiguity clarifications were made on some items and the actual data collection was performed.

Table 1: Cronbach α output for the original measure, pilot study, and main study

Scales & sub-scales		No of items	Original Measure	Pilot study	Main study
BFFI	Openness	6	.81	.90	.91
Sub-	Conscientiousness	6	.86	.87	.88
scales	Extraversion	6	.83	.91	.93
	Agreeableness	6	.89	.84	.87
	Neuroticism	6	.87	.75	.92
	BFFI-total	30	.85	.81	.91
ISPS		18	On ave., .79 - .86	.89	.94

Source: SPSS output

2.6. Data Collection Procedure

The five data enumerators (one per major stratum) were purposively recruited and familiarized with the data collection instruments. The recruitment procedure assumed their InfoSec research practice (data collection, and analysis experience activities across national organizations. Convenience during data collection time was also another additional criterion for selecting them. Considering their experience, knowledge, and exposure to the data collection practices, the researcher delivered 2 hours of training on how to approach participants, describe the purpose of the study, take their consents, administer, and collect the questionnaire. The enumerators administered the instruments by hands before the participants started their regular tasks in their office (from 8:00 to 9:30 AM).

Generally, the data collection practice takes place for one month.

2.7. Data Analysis

All data managed using Statistical Package for Social Science (SPSS v.25) software. Generally, a descriptive statistics such as frequency and percentage (for its appropriate nature with the nominal data); and the independent sample t-test, one-way ANOVA, Pearson Correlation Coefficient Matrix, and hierarchical multiple regression *(to control the effect of confounding variables and test the independent or joint contribution of the predictor variables to the dependent variable)* data analysis techniques were employed for their appropriate nature with interval level data and research questions (Marczy et al. (2005) and Raudenbush (2015) Schattner and Mazza, 2015). In addition, assuming its relevance in considering the unequal sample size between groups (Teijlingen and Hundley, 2014), the Scheffe post hoc ANOVA test was employed. It used to identify which mean significantly differs from the other in all significant F values of the univariate analysis. Generally, the statistical significance level of the study was set at alpha .05.

2.8. Data Screening and Test of Model Assumptions

The issue of missing values, extreme values, and data normality assessed through frequency counting, extreme score elimination, and mean replacement techniques. However, 24 questionnaires were dropped out, because they were incomplete and difficult to treat them.

Using histogram and skewness tests, the means were nearly equal and the skewness was within the range of the acceptance level (-1 to +1) for all scales and sub-scales. This implies the data was reasonably normal and the assumption of normality was satisfied (Bernik and Prislan, 2016). Secondly, the scatter plot analysis and statistical significance of correlation coefficients between the IVs and DV tests were employed to examine the assumptions of linearity and resulted $r_{xy} > .30$, implies a good model fit or non-multicollinearity effect between the IV and DVs' (Teijlingen and Hundley, 2014). Finally, homogeneity of variance tested using Levene's test and the values of the test statistic were found $p > .05$, indicates the assumption of equality of variance was satisfied for those scales and sub-scales.

3. Results and Discussion

Table 2: The Demographic Characteristics of Participants (N=296)

Variable	Label	Figure	Percent
Sex	Female	101	34.12 %
	Male	195	65.88 %
Age	Minimum	27 years old	-
	Maximum	36 years old	-
	Average	31 years old	-
Level of education	Diploma	26	8.78 %
	1st degree	218	73.65 %
	2nd degree	52	17.57 %
Work experience	Minimum	2 years	-
	Maximum	10 years	-
	Average	6 years	-
Job position	Junior Employees	265	89.53 %
	Supervisor	19	6.42 %
	Team leader	9	3.04 %
	Director	3	1.01 %
Length of InfoSec training taken	3 days (24 hours)	93	31.42 %
	5 days (39 hours)	116	39.19 %
	6 months	87	29.39 %
	Total N	***296***	***100 %***

Source: Questionnaire data, 2020

Table 2 above showed the demographic data of participants who were able to fill the questionnaire. Based on the population size of the agency and implication of the pilot data, reasonably representative participants were sampled in sex, age, level of education, work experience, job position, and length of InfoSec training taken categories. Accordingly, the data simply confirmed that the researcher can draw inferences about the target population using the sample characteristics.

3.1 Differences in InfoSec Performance by the Sex of Employees

Table 3: Independent t-test of InfoSec performance as a function of employees' sex (N=296)

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		

Source: Questionnaire data, 2020

To test the employees' InfoSec performance as a function of sex, an independent samples t-test was performed. The result revealed that the InfoSec performance of employees significantly differed by their sex [*t* (1, 294) = 17.42, *p* =.00, Cohen's *d* = 2.21]. Generally, the finding illustrated 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 value showed that male employees scored 2.21 standard deviation higher on the InfoSec performance than females. Similarly, Metalidoua et. al. (2014) and McCormac et. al. (2017) found women are more responding to phishing emails or tend to have more susceptible tendencies to lower InfoSec performances. They have a strong desire to open phishing emails and get information beach in their computers than males. However, their finding was based on email phishing, implies total reliance on the electronic forms of InfoSec with excluding physical/printed forms of InfoSec. Therefore, the present study was more comprehensive than the works previous researchers by incorporating and examining the unexamined parts.

Besides, the Levene test result indicated that the assumption for equal variance was assumed [*F* (1, 294) = 27.5, *p* =.88]. This means that the variances in male and female participants were not significantly different or variances in both sexes were approximately equal.

3.2 Employees' InfoSec Performance Differences based on their Level of Education, Job Position, and Length of InfoSec Training taken

Table 4: A one-way ANOVA analysis of InfoSec performance as a function of employees' educational levels, job position, and length of InfoSec training taken (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*
	1st degree	*218*	*41.04*	*5.71*				
	2nd degree	*52*	*56.42*	*4.34*				
InfoSecPerformance	Job Position							
	Ordinary	*265*	*40.62*	*4.59*	*3*	*292*	*46.59*	*.00*
	Supervisor	*19*	*56*	*1.84*				
	Team leader	*9*	*60.33*	*2.18*				
	Director	*3*	*68*	*1.21*				
InfoSecPerformance	InfoSecTraining							
	3 days	*93*	*30.34*	*3.78*	*2*	*293*	*846.19*	*.00*
	1 week/5 days	*116*	*44.07*	*2.19*				
	6 months	*87*	*53.34*	*5.22*				

Source: Questionnaire data, 2020

One-way ANOVA was employed to examine employees' InfoSec performance difference as a function of demographic factors. As a result, the finding revealed that employees' InfoSec performance significantly differed by their level of education, job position, and length of InfoSec training taken [*F* (2, 293) = 217.71, *P* < .05, = .00, η^2= .60], [*F* (3, 292) = 46.59, *P* =.00, = .00, η^2= .324], and [*F* (2, 293) = 846.19, *P* =.00, = .00, η^2= .85] respectively. In addition, the Scheffe post-hoc ANOVA result indicates the presence of significant mean score differences between: [*diplomas and 1st degrees; diplomas and 2nd degree; and 1st degree and 2nd degrees*], [*ordinary employees and supervisors; ordinary experts and team leaders; ordinary experts and directors; supervisors and team leaders; supervisors and directors; team leaders and directors*], and [*employees who took 3 days of InfoSec training and 5 day; 3 days and 6 months; and 5 days and 6 months of InfoSec training*].

Generally, the ANOVA computation illustrated that employees with higher level of education, job position, and length of InfoSec training tend to have better performance to protect the confidentiality, integrity, and availability of information than those of employees having lower education, job position, and length of InfoSec training. This finding confirmed the Tenney et al's (2015) work, stated that employees with higher level of education are less vulnerable to InfoSec problems. As employees educate more and more, they tend to develop pragmatic skills, knowledge, awareness, and practices to keep the information secretly, in an organized and integrated manner, and use it with its intended purpose. Looking the job position, the present study revealed that employees with higher level of job position tend to have higher InfoSec performance than lower-levels. This finding is consistent with the existing body of literature. For example, a study by Shropshir et al. (2006) suggested that managers are more conscious in making the information private and use it properly than the junior employees. They are also more equipped in making the information only accessible to the authorized users. Furthermore, Savola (2015) indicated a moderate association between length of the InfoSec training taken and information confidentiality performance *(r = .58),* which supported by the present finding. This means that employees who took a longer InfoSec training tend to better secure the privacy of any information. However, it was done based on a single dimension of InfoSec triad (confidentiality). Generally, this study provided a self-report and evidence-based understanding of the employees' InfoSec performance difference as a function of their level of education, job position, and InfoSec training taken in the Ethiopian, INSA context.

3.3 The Relationship between the Predictor and Criterion Variables

Table 5: Summary of Pearson Correlations between the participants' age, work experience, personality difference, and InfoSec performance

N=296	Age	W.ex.	O	C	E	A	N	ISP
Age	1							
Work Experience	.54**	1						
O	.13**	.02**	1					
C	.10**	.26**	.294**	1				
E	.23**	.18**	.96**	.33**	1			
A	.11**	.22**	.29**	.75**	.33**	1		
N	.00**	.21**	-.07	-.37**	-.09	-.37**	1	
ISP	.33**	.14**	-.099*	.61**	-.06	-.02**	-.54**	1

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

Pearson correlation coefficient was performed to test the relationship between the predictor and predicted variables. Accordingly, the InfoSec performance scores of employees were positively related with age *(r (294) = .33, p < .01,* r^2 *= .11)*, work experience *(r (294) = .14, p < .01,* r^2 *= .019),* and conscientiousness (*r* (294) = .608, *p* < .01, r^2 = .37; and negatively correlated with scores of openness (*r* (294) = -.099, *p* < .01, r^2 = .009), extraversion (*r* (294) = -.055, *p* < .01, r^2 = .003), agreeableness (*r* (294) = -.018, *p* < .01, r^2 = .0003), and neuroticism (*r* (294) = -.549, *p* < .01, r^2 = .30).

When employees becoming more old, experienced, and conscientiousness (prepared, organized, properly place computer and print files), they tend to maximize the confidentiality, integrity, and availability of information in their hands. This finding was consistent with various research works. For instance, Savola (2015) found that employees with younger ages and lower years of work experience are more susceptible to InfoSec problems than older ages and higher years of experience. McCormac et al. (2017) also found a positive association between conscientiousness and information confidentiality dimension (*r* = .37). In contrast, employees with openness personality type (curious and searching to know about many things), extraversion (having strong interaction, communication, and contact with different peoples and strangers), agreeableness (showing easy acceptance to external influence and persuasion, being trusting others, and trying to be kind for everyone) and neuroticism (lots of mood changes, easy disturbance, and emotional instability) leads to loss files handled in their computer as well as file shelves. This finding supported the research works of McCormac et al. (2017) that openness (*r* = -.18), extraversion (*r* = -.12), and neuroticism (*r* = -.31) as negatively correlated with information confidentiality. Also, Parsons et al. (2015) found a negative association between employees' InfoSec performance and their agreeableness (easily trusting and influenced by others) (*r* = -.01).

Furthermore, concerning on the magnitude of relationship, conscientiousness, neuroticism, openness, extraversion, and agreeableness effects explained 37 %, 30 %, .98 %, .3 %, .0324 % of the total variance in their InfoSec performance scores, respectively. This shows that conscientiousness and neuroticism have moderate effects on the employees InfoSec performance scores, whereas openness, extraversion, and agreeableness have smaller effects. However, the direction of relationship among variables significantly varied. Except conscientiousness, all the remaining variables are negatively corelated with the scores of employees InfoSec performance.

Generally, the present study was consistent with the previous empirical findings discussed above. However, the previous works were done based on single perspective. Therefore, the present study made a significant contribution by incorporating and examining the remaining two InfoSec measuring triads (integrity and availability).

3.4 Predicting the InfoSec Performance of Employees' using the Predictor Variables

Table 6: Summary of the Hierarchical Multiple Regression results of personality difference in predicting the employees InfoSec performance (N = 296)

Model	Variables entered	*Adjusted R^2*	*R^2 change*	*Beta*	*t*	*Sig*	*F*	*P*
1	Openness	.006	.010	-.38	-2.60	.010	2.89	.000
2	Conscientiousness	.423	.417	.99	3.58	.001	19.13	.000
3	Extraversion	.424	.001	-.113	.790	.043	72.79	.048
4	Agreeableness	.444	.024	-3.73	-3.16	.002	59.87	.000
5	Neuroticism	.557	.113	-.37	-8.87	.000	75.15	.000

Source: Questionnaire data, 2020

Hierarchical multiple regression analysis was employed to predict the InfoSec performance of employees using the predictor variables both separately and jointly. Independently, openness negatively predicted the InfoSec performance scores (β = -.38, t (294) = -2.60, p = .00), as did extraversion (β = .790, t (292) = -.113, p < .05), agreeableness β = -3.73, t (291) = -3.16, p < .01), and neuroticism scores (β = -.37, t (290) = -8.869, p < .01). Conversely, conscientiousness scores positively predicted InfoSec performance scores (β = .99, t (293) = 3.583, p < .01). The standardized beta coefficients indicate a change of one standard deviation in the openness, extraversion, agreeableness, neuroticism, and conscientiousness scores result in a change of -.38, -.113, -3.73, -3.7, and .99, standard deviations in the employees InfoSec performance scores respectively. Jointly, the five independent variables (IVs) such as openness, conscientiousness, extraversion agreeableness, and neuroticism predicted the employees InfoSec performance scores (R^2 = .557, F (5, 289) = 65.611, P = .00). Moreover, adding conscientiousness to openness increased the explained variation by (R^2 = .423, F (2, 293) = 19.13, P = .00) as did extraversion by (R^2 = .424, F (3, 292) = 72.79, P = .00), agreeableness by (R^2 = .444, F (4, 291) = 59.87, P = .00), and neuroticism by (R^2 = .557, F (5, 290) = 75.15, P = .00).

In addition to statistically predicting the employees InfoSec performance scores both independently and jointly, conscientiousness scores improved the prediction by (R^2 *change* = .417, F (1, 293) =19.13, p = .00, $f^2 =$ .81), as did extraversion (R^2 *change* = .001, F (2, 293) = 72.796, p = .00, $f^2 =$.001), agreeableness (R^2 *change* = .024, F (4, 291) =59.865, p = .00, $f^2 =$.025), and neuroticism (R^2 *change* = .113, F (5, 290) =75.147, p = .00, $f^2 =$ .13). In terms of magnitude, conscientiousness was highly affected prediction followed by neuroticism, agreeableness, openness, and extraversion (41.7 %, 11.3 %, 2.4 %, 1 %, and 0.1 %) respectively. Hence, the five IVs jointly accounted for 55.7 % of the variance in the InfoSec performance scores of employees in the INSA context. While, 44.3 % of the variance in the employees InfoSec performance was explained by the unknown factors which are not included in the present study.

Generally, the regression analysis of the present finding confirmed the research works of Jain and Pal (2017). According to Jain and Pal, planned and organized behaviors of employees serve as a positive predictor's information confidentiality (showed 31 % and 29 %) respectively. However, as it is mentioned in the above sections, Jain and Pal's have lacked comprehensive nature.

4. Conclusion

Based on the findings of this study, the following conclusions were drawn. First, the employees InfoSec performance significantly differed by their demographic characteristics such as sex, level of education, job position, and length of InfoSec training taken. This implied that as employees educated more, increased in their job positions, and took longer InfoSec training, they tend to acquire more pragmatic knowledge, competencies, skills, experiences, and responsibilities that may help them to keep the information private and protect it from unauthorized deletion, modification. They develop log-in control behaviors for computers, files, and folders; use antiviruses; give priorities for physical access control of any information at work; never share their passwords and file shelf keys even for co-workers etc.

Second, age, work experience, and conscientiousness were positively related with the InfoSec performance of employees in Ethiopian, INSA context. This implied that employees with prepared, preserved, planned, organized, and scheduled personality characteristics feel responsible and worry to protect the agency's information from illegitimate users. Consciously check the source (subject and sender) of both electronic such as email and physical messages. They usually used multiple security control procedures like passwords or locks, encryption, and other security settings. Also, they periodically maintained the database and place of documents in their computer or file shelves to ensure their confidentiality, integrity, and availability. In contrast to age, work experience, and conscientiousness, the openness, agreeableness, extraversion, and neuroticism scores of employees showed a negative association with their InfoSec performance in the same context. This implied that employees with strong curiosity to know many things, interest to try and tackle new challenges; high level of social, interactive, sympathetic feelings; strong need for trusting and pleasing others; and frequent mood shifts, life worries, and stress are unlikely to check and evaluate their files periodically. They have little inclination to use complicated security tools or settings. Rather, they prefer to use simple and guessed passwords, and are more likely to share them with other people around them. Accordingly, the files, manuals, or any workplace information in their hands may be easily exposed, lost, deleted, changed, modified, or even could be unavailable to the right customers.

Finally, the findings of this study revealed that the five predictor sub-variables significantly predicted the criterion variable both independently and jointly. That is, independently 1 %, 41.7 %, 0.1 %, 2.4 %, and 11.3 % of the variance in the employees' InfoSec performance was accounted for by a unit of change in the employees' openness, conscientiousness, agreeableness, and neuroticism scores respectively. Jointly, 56.8 % of the variance in the employees' InfoSec performance was accounted for by a unit of change in the employees' openness, conscientiousness, agreeableness, and neuroticism scores together. However, 43.2 % of the variance in the employees' InfoSec performance was explained by the unknown factors which were not included in the present study.

Generally, even though the data of the present study was entirely self-report and has vivid limitations such as response bias, social desirability effect, and other defects, it contributes a context and evidence-based understanding about the association between personality difference and InfoSec performance of employees in the Ethiopian, particularly INSA context.

5. Recommendation

- ➢ INSA's human resource recruiters and psychometricians recommend to consider candidates with higher conscientiousness personality type when they hire for InfoSec-related job positions.
- ➢ Employers and organizations working with InfoSec-related areas are advised to review the implications of relevant theories, models, and empirical evidence about personality difference and InfoSec performance, so that, they can easily recruit, hire, and place the right personnel to the right positions.
- ➢ Psychologists, trainers, or interventionists working with the InfoSec performance areas need to focus on the influence of personality difference on the employees or users InfoSec performance, and they need to design trainings having an appropriate content and magnitude for users with different personality types.

5.1 Recommendations for Future Research

- ✓ Better to conduct by expanding its scope or incorporating more demographic variables such as type of discipline participants studied, colleges/facilities, and other psychological variables.

6. Limitation of the Study

- ➢ Due to COVID-19 pandemics, the data of this study was entirely self-report and was not triangulated with interviews, Focus Group Discussions (FGD), observation, and other data sources, rather it was full of self-report data.

7. Funding

- ➢ The authors have no funding to disclose

8. Conflict of Interest

- ➢ The authors declare they have no conflict of interest

References

Ajay, S., & Micah B. M. (2014). Sampling techniques & determination of sample size in applied researches: *International Journal of Economics, Commerce, and Management*, *11 (2),* 89-99

Alavi, R. (2016). *A Risk-Driven Investment Model for Analysing Human Factors in Information Security*. Doctoral Thesis, University of East London

Albladi, S. M., & Weir, G. R. (2014). *Personality Traits and Information- Attack Victimisation.* Department of Computer and Information Sciences University of Strathclyde Glasgow, UK

Albladi, S. M., & Weir, G. R. (2017). Personality traits and cyber-attack victimization: multiple mediation analysis. *Journal of Computer and Information Sciences, 54 (5), 354-365*

Alhassana, M. M., & Adjei-Quayeb, A. (2017). Information security in an organization. *International Journal of Computer (IJC), 24 (1),* 100-116

Alvi, M.H. (2016). *A manual for selecting sampling techniques in research*. University of Karachi: Iqra

Bansal, G. (2011). *Security concerns in the nomological network of trust and big5:* 1st order vs. 2nd order: Proceedings of the 32nd International Conference on Information Systems, Shanghai

Bernik, I., and Prislan K. (2016). Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. *Journal of Medicine and Computer Science.*

Computer Security Institute (CSI), (2007*). Computer security and crime survey.* Greenwich

Dhamani, K.A., & Richter, M. S. (2011). Translation of research instruments: research processes, pitfalls, and challenges. *Africa Journal of Nursing & Midwifery, 13(1),*3-13

Geers, K., (2011). Stratagic Cyber Security. North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Tallinn, Estonia

Henry, W., Glaspie, H. W., & Karwowski, W. (2018). Human factors in information security culture: A literature review. *Conference Paper in Advances in Intelligent Systems and Computing, 78 (7).* DOI: 10.1007/978-3-319-60585-2_25

Hinson, G. (2003). Human factors in information security. *International Journal of Research in Information Security Management (IJARM)*, *5 (2).* DOI: 10.2139/ssrn.3205035

Information Security Risk Assessment Team (2019). *An assessment of information security practices, trends, and performance of employees in INSA.* Addis Ababa, Ethiopia

International Organization for Standardization (ISO) 31000 (2018). *Risk management.* Geneva

Jain, J., & Pal, P. R. (2017). A recent study over information security and its elements. *International Journal of Advanced Research in Computer Science, 8 (3),* ISSN No. 0976-5697

John, O. P., & Srivastava, S. (1999). *The big-five personality trait taxonomy*: History, measurement, and theoretical perspectives.

Lapsley, D. K., & Hill, P. L. (2009). Subjective invulnerability, optimism bias, and adjustment in emerging adulthood. *Journal of Youth Adolescence.* DOI: 10.1007/s10964-009-9409

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel Psychology, 28* (4), 563-575.

Metalidoua, E. B., Marinagic, C., Trivellasc, P., Eberhagen, N. B., Skourlasd, C., & Giannako, G. (2014). The human factor of information security: Unintentional damage perspective. *Journal of Social and Behavioral Sciences, 147,* 424 - 428· DOI: 10.1016/j.sbspro.2014.07.133

Michael, M., Dumitras, T., Prakash, A. B., Subrahmanian, V. S., & Wang, B., (2016). Understanding the relationship between human behaviour and susceptibility to information security: *Journal of applied psychology, 114 (12),* 455–463

Nelson, C. & Yorke, L. (2015). The 5-factor model: Investigating personality & accident involvement. *Journal of Prevention & Intervention in the Community*, *35 (28),*99-114.

Parson, K., McCormac, A., & Ferguson, L. (2010). *Human factors and information security:* Individual, culture, and security environment. Control, Communications, and Intelligence Division Defence Science and Technology Organisation: Australia

Pouransafar, M., Maroop, N., Ismail Z., & Cheperli, M. (2015). Review of information security vulnerability: Human perspective. *Journal of advanced informatics school, 56 (34),* 214 -225

Raudenbush, S. W. (2015). *Correlation, hierarchical regression, and experimental designs.* Michigan State University: Lansing

Salgovicova, J., Prajova, V. (2012). Information security management. *Journal of science and technology, 45 (20).* DOI 10.278/v10186-012-0019-0

Savola, R. M. (2015). Towards a taxonomy of information security metrics. *Journal of Information Security Management and Measurement, 7 (4), 78-89*

Schattner P, and Mazza D., (2015). Importance of doing a pilot study. *Journal of Malaysian Family Physician, 5 (8),* 70-73

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M., (2006). *Personality and IT security:* An application of the five-factor model. *Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL)*

Taherdoost, H., (2016). Sampling methods in research methodology: How to choose a sampling technique for research. *International Journal of Academic Research in Management (IJARM)*, 5 (2), 178-188. DOI: 10.219/ssrn.3205035

Taherdoost, H., (2017). Determining sample size: How to calculate the survey sample size. *Journal of Economics and Management Systems, 67 (45),* 235-248

Teijlingen, R., and Hundley, V., (2014). Why a pilot study? *Journal of Applied Psychology.*

Uffen, J., Guhr, N., & Breitner, M. H. (2013). *Human behaviour and information security management.* Institute of Information system: UK

Wendy, W., & Gunawan, W. (2019). Measuring information security and cybersecurity on private cloud computing. *Journal of Theoretical and Applied Information Technology, 96 (1),* 12-22

Zelt, S, Recker J, Schmiedel T, vom Brocke J (2018). Development and validation of an instrument to measure and manage organizational process variety. *Journal of PLoS ONE* 13 (10): DOI: 10.1371/0206198