Running Head: PERSONALITY DIFFERENCE & ATTITUDE ASSOCIATED WITH EMPLOYEES' PERCEIVED INFORMATION SECURITY PERFORMANCE

Addis Ababa University

College of Education and Behavioral Studies

School of Psychology

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

Anemut Mehari Berhanu

November, 2020

Addis Ababa University

College of Education and Behavioral Studies

School of Psychology

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

This thesis report is submitted to the School of Psychology of Addis Ababa University in partial fulfillment of the requirement for the Master of Arts Degree in Social Psychology.

Anemut Mehari Berhanu

Advisor: Dame Abera (Ph.D.)

September 2020

Addis Ababa, Ethiopia

Declaration

I, the undersigned, hereby declare that the thesis entitled, Personality and Attitude Difference Associated with Information Security Performance of Employees in INSA, is my original work under the guidance of Dr. Dame Abera. Also, the thesis contains no material previously published by any other person except where proper citation and acknowledgment has been made. I do further confirm that this thesis has not been presented or being submitted as part of the requirements of any other academic degree.

Anemut Mehari Berhanu

Signature _____

Date _____

This thesis has been submitted for examination with my approval as a supervisor

Dame Abera (PhD)

Signature _____

Date _____

Addis Ababa University

College of Education and Behavioral Studies

School of Psychology

Personality Difference and Attitude Associated with the Perceived Information Security Performance of Employees in INSA

Anemut Mehari Berhanu

Approval of the Board of Examiners

1. Advisor

   Name_____Signature_____Date_____

2. Internal Examiner

   Name_____Signature_____Date_____

3. External Examiner

   Name_____Signature_____Date_____

Abstract

The major purpose of this study was to assess the association between employees' personality difference, attitude, and perceived information security (InfoSec) performance in the INSA context. Accordingly, the five-factor personality differences (OCEAN) and attitude were treated as the independent variables, while the perceived InfoSec performance was treated as a dependent variable. A correlational research design was employed. A total of 320 participants were selected using a stratified random sampling technique. The BFFI, AIS, and ISP scales were administered to collect the quantitative data. The Independent t-test, one-way ANOVA, Pearson Correlation, and multiple regression data analysis methods were performed to address the research questions. Accordingly, the present study revealed the following findings. First, the majority of the employees have higher perceived InfoSec performance in the INSA context. Second, employees perceived InfoSec performance significantly differed by their sex, educational levels, job positions, and length of InfoSec training. Third, age, work experience, personality difference, and attitude were significantly related to the perceived InfoSec performance of employees' in the Ethiopian, INSA context. Fourth, employees' personality difference and attitude significantly predicted their perceived InfoSec performance both independently and jointly. Generally, personnel recruiters, employers, trainers, and interventionists were recommended to consider their candidates' or customers' background characteristics, personality difference, and attitude when they provided their services.

Acknowledgments

First, I would like to thank my research advisor Dr. Dame Abera, for his technical, constructive, academic comments, and follow-ups throughout the whole process of the study.

Second, my thanks go to the officials of the Information Network Security Agency (INSA) particularly the agency director for their permission to conduct the study in the agency and Human Resource Management Department staffs, for their cooperation to provide important information regarding the size, gender, etc. of the target population in the agency.

My special thanks also extended to all the participants of the study, for their kind willingness, consent, and genuine response to the questionnaires. Also, I thank them for properly filling and back the instruments.

My gratitude also goes to all instrument panelists, for devoting their time to validate the instrument and data enumerators, for managing all the data collection practices.

Lastly, I would like to present my heartfelt thanks to all my parents and siblings, for their financial support and encouragement throughout the study.

Table of Contents

List of Tables

List of Acronyms and Abbreviations

CIA - Confidentiality, Integrity, and Availability

InfoSec – Information Security

INSA - Information Security Network Agency

OCEAN - Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism respectively

BFFPI - Big Five-Factor Personality Inventory

AIS - Attitude towards Information Security

PA-ISP - Pattinson and Anderson Information Security Performance

List of Appendix

Chapter One

Introduction

1.1. Background of the Study

Among the different psychological constructs that influence the perceived information security (InfoSec) performance of employees in any organization or settings, personality difference and attitude play a significant role. Regarding this, Ahlan et. al. (2015) and Albladi and Weir (2017) organizational data, information, or files in the world are pervasively dependent on and directly operated by their employees. In this process, particularly when sending, receiving, storing, and using it, the confidentiality, integrity, and availability (CIA) of the information have a great chance to be threatened by the operator's personality trait difference and attitudes. Therefore, this study was designed to assess the association between personality difference, attitude, and perceived InfoSec performance of employees in the Information Network Security Agency (INSA) context.

In this study context, 'perceived InfoSec performance' implies the data is based on the self-report, views, or perception towards own performance rather than using the actual day to day measures of their InfoSec performance. It is the employees' personal view or perception towards their own InfoSec performance such as the ability to keep any workplace information, file, or documents confidential, secured, remain unchanged, and rightly available to the authorized users. It can be referred to as the use of a strong computer as well as folder passwords, file shelf keys to protect the files from unauthorized changes, deletion, modification, or lost when storing, sending, or receiving (Alhassana & Adjei-Quayeb, 2017).

The issue of InfoSec performance is not a single matter of Information Technology (IT); it's now a critical success factor for the whole organization because, organization managers have discovered that information is one of the most valuable assets like every physical asset that must be protected (Tenney et. al., 2015).

In human history, several personal, organizational, national, and even world level information have been reached to unauthorized users either deliberately or non-deliberately and used for manipulation of the targets. In all those information insecurities or threat activities, humans with their various psychological factors are the significant role players (Hadlington, 2017).

Even if the employees' personalities are numerous, in this study, only personality differences which comprise of openness to experience (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) and attitude towards InfoSec are emphasized. Because, different researchers (e.g., Bansal, 2011; Campbell et. al., 2010; and Uffen et. al., 2013) suggested the positive value of personality difference particularly conscientiousness and positive attitude towards InfoSec policy compliance on organizations as well as employees InfoSec effectiveness. Also, the big five personality factors and attitudes are considered to be the leading models for measuring and understanding personality difference and attitude associated with InfoSec performance issues. But still, now there is a controversy regarding the association and prediction between these three variables.

On the other hand, the five-factor personality type model explained, users' InfoSec performance can be best predicted by the personality type that they have. For example, conscientiousness (traits of thinking before acting, following norms and rules) associated with high InfoSec performance, while neuroticism, extraversion, agreeableness, and openness are usually associated with low InfoSec performance of employees (Eber & Ttsuoka, 2016; and McCrae, 2017). Also, in the Knowledge, Attitude, and Behavior (KAB) model of Kruger and Kearney (2006) users' positive attitude towards InfoSec is positively associated with high InfoSec performance, because attitude can have a significant impact in guiding users' behavior. If users have a positive attitude towards InfoSec related issues, then they have a high tendency to behave by achieving a high InfoSec performance.

Different scholars defined InfoSec performance differently. For example, Salgovicova and Prajova (2012) defined InfoSec performance is the capability to protect the confidentiality, integrity, and availability of computer system data from those with malicious intentions. Whereas Wendy and Gunawan (2019) defined first, InfoSec is all about user's interaction with any information in their hands or devices; then after InfoSec performance is the user's ability to keep its confidentiality, integrity, and availability when sending, receiving, and storing it either physically or electronically. For example, using strong passwords for computers, folders, and documents and changing it in three or fewer month's intervals having electronic or non-electronic file backups for every information, etc.

However, in the present study, the researcher is interested to assess it compressively, which is both physical (e.g. printed documents) and electronic information (e.g. computer system). Meaning, InfoSec is an employees' successful ability in sending and receiving any information using a trusted system (e.g. INSA's internal Dagu email), storing any information in a secured and strong passworded computers, places, or locked shelf. Because, Carlos (2002) indicated that, by measuring such employees' successful activities, we can compressively assess their perceived InfoSec performance in the CIA triads.

In this regard, confidentiality refers to successfully keeping, storing, and transferring the information to the expected authorized users with preserving it from unauthorized access, for example, by setting strong passwords, put documents in a very secured place, etc.; integrity refers to successfully protecting the information from the unauthorized users' modification; and availability focus on the ability to make the information timely available to the authorized users when it's needed.

As we live in the information era, our daily life is becoming increasingly dependent on the information and its security issues (confidentiality, integrity, and availability) (Alavi, 2016). Accordingly, Kaur & Mustafa (2013) implied, the greater connectivity, information sharing, and storing practice resulted in increased InfoSec vulnerability or threats. But, the vulnerability of the information varies from person to person or organization to organization.

Regarding this, researchers (Ahlan et. al., 2015; Albladi & Weir, 2017; Karwowski & Glaspie, 2018; and Mekovec & Hutinski, 2015) tried to focus beyond the users' InfoSec related knowledge, skills, and awareness and show us the crucial roles of individuals personality type differences and attitudes in predicting InfoSec performances. But the literature survey has shown that most attitude studies lacked comprehensiveness. For example, Gundu (2015); Pervin & John (2016); and Pouransafar et. al., (2015), examined it only from an organizational InfoSec policy compliance perspective, rather than assessing it from cognition or thought, feeling, and behavioral perspectives about InfoSec practices and policy compliances.

Studies in the United States and Europe by different researchers such as Lapsley and Hill (2009), Metalidoua et. al., (2014), and Parson et. al. (2010) indicated the challenges associated with InfoSec are far from resolved. Most of the employees' InfoSec performance problems are attributed to be the lack of sufficient budget allocated for InfoSec and poor technical knowledge and skills rather than the attitude towards InfoSec and emphasis given to organizational information confidentiality, integrity, and availability, and personality type differences.

Employees with low InfoSec performance in organizations can cause financial losses, disruption of business, services, productions, and even mental health disturbance and loss of life in the case of health institutions (Taherdoost, 2017). A significant statistic found by Ada et. al. (2009) showed, due to InfoSec threats, 194 organizations in the US lost approximately 66,930,950 $ in a single year. Interestingly, up to 20% of loss is assumed to be psychological errors of the internal users/ employees (e.g., weak compliance with organization InfoSec policies).

Currently, different InfoSec performance improvement standards and policies have emerged in organizations, but the InfoSec performance problems of employees in the world are becoming pervasive and increased from time to time. For example, a Computer Security Institute (2007) found that 46% of the 487 participants in their organizations are exposed to at least one InfoSec incident problem in a given 12 months. While in 2012 reported, 49 % of 512 participants were exposed to an average of two information confidentiality losses in a single year. Besides, a very recent study by Jain and Pal (2017) found, nearly 56 % of users in the organization have lost their electronic (e.g., computer, e-mail) information confidentiality by unauthorized users. All these three findings directly implied that InfoSec performance problems are beyond the technical skills, knowledge, and awareness of the users/employees.

For many years, to improve the InfoSec performance of employees, organization directors worked hard on their InfoSec skill developments or hired competent InfoSec experts. But such acts do not fully ensure the organizations as well as its employees' InfoSec performance, because InfoSec performance is something that additionally requires the security focus, organized, and higher-level risk perceiving traits of the users. An important issue here is that employees' attitude towards information confidentiality, integrity, and availability are little researched except in the confidentiality dimension, and little emphasized even by most InfoSec focused organizations (McCormac et. al., 2017; and Uffen et. al., 2013).

Similarly, most researchers intensively studied and consistently reported a lack of users InfoSec awareness is the number one obstacle in achieving a good InfoSec posture (Shropshire et. al., 2006; Taherdoost, 2016 and 2017). Continuous and periodic InfoSec awareness training activities were delivered to ensure the InfoSec performance of themselves as well as the organizations and reduce the issue of InfoSec threats. Even if users' InfoSec awareness level has been grown, organizations and users cannot achieve their maximum InfoSec performances.

An awareness of InfoSec is the vigilance of understanding and perception of various InfoSec threats.

However, an understanding of threats alone seems insufficient to motivate one to take actual actions in preventing InfoSec problems. Also, achieving an optimum InfoSec performance is beyond the technical aspect of InfoSec awareness rather it incorporates the security-sensitive personality types and positive attitude of the users (Ajay and Micah, 2014; and Uffen et. al., 2013).

In Ethiopia, InfoSec problem incidents are still very prevalent, have seen an exponential annual increase, and work hard to improve the InfoSec awareness levels of users in different federal level governmental offices. According to the agency's Information Security Risk Assessment Team (2019) report, there were near twice as many InfoSec incidents than in 2015. Nine out of ten InfoSec threat incidents are roughly attributed to some sort of employees' errors (e.g. lack of InfoSec awareness). Also, a 9 % increase in employees' involvement in InfoSec threats has been reported from 2017 to 2019. Finally, it suggested that employees in the agency may have a weak link in InfoSec issues.

Given the complex explanations given by different scholars about the issue under study, the researcher presented an empirical finding on how personality difference and attitude associated with the perceived InfoSec performance of employees in Ethiopia, particularly in the INSA context.

1.2. Statement of the Problem

As we live in the information age and continuous advancements of technology, we send, receive, share, and store a bulky amount of critical personal and organizational information such as files, documents, etc. in our everyday life (Salgovicova and Prajova, 2012). To maintain the confidentiality, integrity, and availability of the information, most organizations lacked to focus on and cultivate their employees' personality differences and attitudes towards InfoSec related issues. Rather, they are solely tagged to improve users' InfoSec awareness, skills, and knowledge. Surprisingly, InfoSec is not solely a technical issue, it has also human psychological aspects such as personality difference, attitude, and others (Wendy and Gunawan, 2019). Regarding this, Karwowski and Glaspie (2018) found, more than 90% of employees' InfoSec threats in an organization setting is due to their non-security conscious personality traits, negative attitude towards InfoSec, and other psychological factors.

In earlier studies, InfoSec researchers have anticipated the relationship between personality difference and the user's InfoSec attacks such as social engineering-based attacks. But, now a day, some research has empirically examined the impact of personality differences on InfoSec threats such as email phishing response and loss of one's InfoSec. However, the effect of users' or employees' personality difference on their InfoSec performance is still a controversial topic in InfoSec research. Because, Jain and Pal (2017) stated that neuroticism is the only personality type that negatively correlated to phishing email responses resulted in information loss, while Pouransafar et. al. (2015) presented opposing findings in that openness, extraversion, and agreeableness personality types significantly increased the user's tendency to comply with phishing email requests and engage them to high-level information loses.

Also, Iasi (2016) studied the link between sales employees' attitudes and their information confidentiality performance and found a strong positive relationship (r= .71). However, Flowerday (2016) investigated the same issue and found a very weak relationship *(r = .002).* In these studies, first, both the researchers didn't show us how much of the variance in employees' information confidentiality performance is predicted by their attitude. Second, they investigated the association between those variables using a single InfoSec behavior (confidentiality) dimension, rather than using all the 3 InfoSec performance components. Therefore, considering these two research gaps, in this research, the researcher is going to relate and predict attitude and InfoSec performance using a compressive (CIA) InfoSec performance measure model.

Regarding Alhassana and Adjei-Quayeb (2017) suggestion, critical organizations such as banks, land management, and mapping work offices have a higher level of InfoSec threats and the chance of being targets of information fraud attackers, because they are assumed to have a national and even world level critical information about the physical, economic, political, social, geographical/territorial aspects of the country. Based on the criticality of the information exposed to unauthorized users, nations or organizations may experience serious social, economic, cultural, and political problems, or even they may fail or disrupt. In line with this, Computer Security Institute (2013) statistics in Europe and America shown that almost 19 private or governmental, civic or profit, economic, social, or political organizations have been stopped their normal functioning, become stagnant, totally failed, or replaced by other new forms in every 2 or 3 years.

In Ethiopia, some organizations have faced nearly the same experiences. For example, in 2016, the Ethiopian Management Institute had lost all the data/information accumulated in its database system. According to the institute Risk Assessment Committee /RAC (2016) report, more than three challenging months were taken to feed the fragmented data into the system again. Besides, the institute has lost approximately 849, 514.24 birrs. Lastly, the committee report indicated that some users including the IT staffs in the institute were carelessly used the database system and its information e.g. repeatedly used and left the workroom without logging off the system and their computer, because, they were believed that, nothing will happen to the information that they managed in their computer and nobody will target them for information fraud.

A simple assessment of the general InfoSec practice and trends of employees in INSA conducted by Risk Assessment Team (2019) has concluded that nearly 93 % of the participants have strong InfoSec practices, while the remaining 7 % have weak practices. This means that employees' can not simply open and respond to an email request from the unknown source, did not use easily guessed passwords, change their passwords regularly, and did not randomly put the printed files. But this finding is completely contradicted with reports of the agency's Computer Security Team (CST) and Logistics Management Team (LMT) (2019). According to these teams' report, due to the unsecured characteristics when sending, receiving, and storing any data/information e.g. making the information easily accessible to unauthorized users, corrupting, and deleting files, nearly 9 to 13 desktop computers become out of service and back to storerooms in each year. This figure directly implied that there is a weak InfoSec practice of employees in the agency.

The major gap observed in these two assessments was that first, they were focused on the lack of employees' InfoSec practices. Second, the employees' variability in sex, age, work experience, job position, educational level, length of InfoSec awareness training, personality, and attitude related to their InfoSec practice remained unexamined.

Besides, in 2018/2019, some documents containing the internal structure and functioning of the agency (INSA) were taken by unauthorized users and used for the unintended purpose in social media (e.g. Facebook). Due to this, the internal staff of the agency were faced with negative psychological problems such as tensions, distrust between co-workers, and difficulty of working in teams. This event was also little affected the regular functioning of the agency.

Finally, when the issue was investigated internally, it was found to be the errors of some staff who were responsible in particular to those materials. They have assumed the materials are not the targets of information confidentiality attackers and put them in a little secured place. When asked, one responsible staff was responded as *"I feel and think that nobody will target the materials".* Roughly, this is indicated how much of the staff(s) attitude towards InfoSec brought massive psychological, social, and political problems.

Moreover, different researchers such as Iasi (2016); Joseph (2016); Mekovec and Hutinski (2015); Pattinson et. al. (2015) studied personality difference, attitude, and InfoSec performance for own objectives. However, 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. Generally, considering the literature gaps mentioned above and the need to fill those gaps using empirical data in the Ethiopia, INSA context, the researcher has designed the following research questions.

1.3. Research Questions

In this study, the researcher attempted to answer the following basic research questions:

RQ₁. What is the level of employees' perceived InfoSec performance in Ethiopia, INSA context?

RQ₂. Does the perceived InfoSec performance of employees vary as a function of their sex, level of education, job position, and length of InfoSec training taken in Ethiopia, INSA context?

RQ₃. Do age, work experience, personality differences and attitudes significantly relate to the perceived InfoSec performance of employees in Ethiopia, INSA context?

RQ₄. Do personality differences and attitudes significantly predict the perceived InfoSec performance of employees in Ethiopia, INSA context?

1.4. Purpose of the Study

The major purpose of the current study was to assess the association between personality differences, attitude towards InfoSec, and perceived InfoSec performance among employees in INSA.

More specifically, it intends to: -

- To identify the level of employees' perceived information security performance in the INSA context
- Assess the personality difference, attitude towards InfoSec and InfoSec performance of INSA employees vary as a function of age, sex, work experience, level of education, job position, and length of InfoSec training taken.
- Investigate the relationship between the personality difference, attitude towards InfoSec, and InfoSec performance in the INSA context.
- Examine the hierarchical prediction of personality difference and attitude towards InfoSec on InfoSec performance in the INSA context.

1.5. Significance of the Study

The findings of this study will have the following significance.

First, it will help the agency as well as other organizational managers, administrators, and employees to acquire adequate empirical or evidence-based knowledge about the influence of personality difference and attitude on InfoSec performance. As a result, they may benefit to improve their InfoSec performance through aware of and managing their big-5 personality trait weakness related to InfoSec and developing an appropriate positive attitude towards InfoSec policies, proclamations, and standards.

Second, the findings of the study will help the curriculum and course developers and InfoSec related policy planners, to design an integrative curriculum, courses, and formulate policies with incorporating issues of personality differences and attitudes.

Third, the findings of the study will help InfoSec trainers to design an integrative training manual with incorporating the impacts of big-5 personality traits and attitude. As a result, the individuals, as well as organizations, may reduce information security threats that come through the issues of personality trait difference and attitude through awareness of and managing it.

Fourth, the findings of the study will suggest the personnel recruiters as well as hiring organizations to recruit and hire the right personnel for the right InfoSec position, using the personality trait difference and attitude measures.

Fifth, the findings of the study may also benefit researchers in drawing clear insights about employees' personality differences and attitudes that affect their perceived InfoSec performance INSA context.

Similarly, the findings of the study may open the way for indigenous researchers to include more psychological variables and examine their effects on the issues of the organization as well as individuals' perceived InfoSec performance.

1.6. Delimitation of the Study

As it is mentioned in the previous sections, this study was delimited to employees in Information Network Security Agency (INSA). Here, employees refer to 2019/2020 active workers in the agency. The agency was found in Lafto Sub-city, District 4, Bisrate Gebril.

Also, psychological factors consist of numerous constructs, but in this study, only personality differences and attitudes towards InfoSec were investigated. Additionally, perceived InfoSec performance was examined as a predicted variable.

Finally, even if there are numerous socio-demographic variables such as economic status, ethnicity, residence, etc., in this study, only employees' age, sex, work experience, educational background, level of education, job position, and length of InfoSec training taken were considered and examined due to the issues of practicality and resource limitations.

1.7. Limitation of the Study

Generally, this study has two major limitations:

- Due to the agency's working culture and issues of security, the researcher can not personally observe the information security performance of the employees in their working rooms.
- Due to time and difficulty of managing all things by the researcher potential, the data was not triangulated with the interviews, Focus Group Discussions (FGD), and other data sources, rather it was totally dependent on the perceived self-reports data of the employees.

1.7. Operational Definitions of Terms

In this study: -

- ***Personality***: refers to a collection of consistently shown features or a relatively enduring and unique pattern of thinking, feeling, behaving, or characteristics of an employee that differentiate him/her from others.
- ***Personality difference:*** is defined as the differences in the combination of the big five dimensions of personality called openness to experience, conscientiousness, agreeableness, extraversion, and neuroticism (OCEAN). Numerically, it refers to the total score of the respondent's responses in each sub-scale of the adapted John and Srivastava (1999) Big-5 personality inventory.
    - **Openness to experience:** employees' inherent and flexible personality characteristics, approaches, interests, or trials towards new experiences.

- **Conscientiousness:** employees careful, organized, planned, hard-working, determined, achievement-oriented, decisive, and disciplined personality traits.
- **Extraversion:** employees sociable, being full of life, excited, cheerful, talkative, enterprising, experiencing positive feelings, and joyful personality traits.
- **Agreeableness:** employees' kindness, trustworthiness, caring for others, forgiving, tolerant, compromiser than the competition, helpful, and interpersonal conflicts avoidant personality characteristics.
- **Neuroticism:** employees' negative emotions such as nervousness, anxious, needing the approvals of others, suspicious, constantly changing moods, and being inconsistent personality characteristics.

- ***Attitude*** refers to favorable or unfavorable feelings, behaviors, and thoughts that an employee has towards InfoSec related issues and practices. Numerically, it refers to the total score of the respondents' responses on the Ahlan et. al., (2015) attitude towards InfoSec (AIS) measure scale.
- ***Information*** refers to an organized form of any physical/printed or electronic/computer files, documents, manuals, research outputs, reports, knowledge, or facts provided or learned about something or someone that obtained from study or instruction.
- ***Security*** refers to a practice or behavior of preventing or prohibiting the information from unauthorized users.
- ***Perceived Information security (InfoSec)*** is the employees' view or perception towards their ability to protect any workplace electronic or non-electronic data, files, or documents from the unauthorized disclosure, unauthorized deletion, modification, change, or add, and timely present to the authorized users. In other words, it refers to the perceived ability of an employee to keep, store, and use the information confidential, integrated, and available. Numerically, it refers to the total score of the respondent's responses on the Pattinson and Anderson (2007) perceived InfoSec Performance Measure Scale (PA-ISPS).

Chapter Two

Review of Related Literature

In this chapter, the concept of personality differences, attitudes, and information security performance was discussed in detail. Also, employees' personality differences and attitude and their association with the InfoSec performance of employees were discussed. Finally, the conceptual framework of the study, implications of the literature, and summary points were presented.

2.1. Personality Difference

Since this time is an information age, the organization having the right information at the right time will succeed against its competitors. To ensure the continuity of the organization with minimizing its business damages and maximizing its return on its service or business opportunities, it must have employees with good InfoSec performance. Because it protects the organization's information or any work files from a wide range of threats and losses. Therefore, to achieve good InfoSec performance, organizations must consider their employee's personalities, attitudes, and other psychological constructs (Hadlington, 2017).

Personality is the accumulation of unique characteristics of a person that affects his/her cognitions, motivations, and actions in various ways (Aellik, 2016). A person's unique characteristics can significantly affect and determine his/her perceived information security performance and become the concern of researchers (Alavi, 2016).

Personality differences are personality traits differences based on the five personality dimensions called openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism. This means that differences in personality traits or characteristics that represents an employee holistically, uniquely affect their perception, behavior, and identify performances of InfoSec. It also plays an important in determining the reaction and responses towards perceived InfoSec performances (Albladi & Weir, 2014).

Due to their unique personality characteristics, different individuals are expected to behave and perform differently across various work as well as other settings (Eber & Ttsuoka, 2016). To understand and explain the construct of personality differences, researchers with varying justifications, conceptualizations, consideration of the widespread appeal, range of

applications, and standards have proposed different personality frameworks. However, the big-5 model of personality is a leading theoretical model and widely used model in contemporary psychology (Allport, 1937).

The development of the big five-factor model began with the work of Allport and Odbert (1936), in which some 18,000 personality-related terms were identified. By 1945 the list had been reduced to 35 variables. Following repeated validations, they eventually became known as the big-5 strong factors (Nelson and Yorke, 2015).

Since the inception of the big-5, numerous similar five-factor models were proposed, including models of Botwin and Buss (1989), Costa and McCrae (1985), Goldberg (1981), and Conley (1985). However, one of the most commonly cited models is the big-5 personality trait taxonomy which is suggested by John and Srivastava (1999). It includes factors of extraversion, agreeableness, conscientiousness, neuroticism, and openness. It is also proposed as a means of identifying individuals who are most likely to demonstrate InfoSec related behavior (Mohannak and Alfawaz, 2014).

As Aellik (2016) and John and Srivastava (1999) indicated, choosing the big five-factor model has two salient advantages over other specific factors. One is its inherent generalizability nature in its systematic and comprehensive approach to personality. That is, the factors are not meant to represent a specific theoretical perspective, but rather a complete taxonomy of terms which allow individuals to describe themselves and others. The issue of generalizability permits the use of the model across many research disciplines, including InfoSec performance fields. The second advantage of using the big-5 personality model is that the behavioral patterns associated with the factors are well known in comparison to a large number of specific factors.

Besides, the big-5 personality model has long been used to interpret and predict various factors in diverse environments (Aellik, 2016). For example, it's applied in organizational innovation, human resources management, relationship stability, self-managed workgroup participation, etc. In the InfoSec research realm, progress has been shown towards correlating big-5 personalities with the critical aptitudes that individuals must possess for successful InfoSec performance areas (Nelson and Yorke, 2015) and utilizing its metrics for InfoSec candidate selection (John and Srivastava, 1999).

2.1.1. Openness to Experience

Openness to experience describes the breadth, depth, originality, curiousness, and complexity of an employee's mental and experiential life. Employees who are open to experience are flexible about the principles, try different approaches, and show inherent interests in new experiences. Employees with the openness type are highly trials, imaginative, creative, curious, and courageous, whereas employees who are not open to experience show strong adherence to the organization information security rules, principles, policies, procedures, do not like adventure, show absolute obedience to authority, preferring conventional patterns of working (Karwowski and Glaspie, 2018).

High scores in the openness personality type indicated the creative, curious, sensitivity, trial characteristics of an employee, while the low scores indicated being conventional or conservative and indifferent characteristics of employees to manage the confidentiality, integrity, and availability of workplace information (Bansal, 2011).

2.1.2. Conscientiousness

Conscientiousness describes a socially prescribed impulse control that facilitates task and goal-directed behavior of an employee, such as thinking before acting, delaying gratification, following norms and rules, and planning, organizing, and prioritizing tasks. Employees with high scores of conscientiousness personality type are highly careful, organized, decisive, scheduled, hard-working, determined, achievement-oriented, decisive, orderly, well organized, prepared to deal with any workplace problems, adherence to ethical principles and values (Alavi, 2016; and Grazziano, 2015).

2.1.3. Extraversion

Extraversion implies an energetic approach towards the social and material world, including traits such as sociability, activity, assertiveness, and positive emotionality. Employees with dominant extraversion personality tend to be outgoing, active, ambitious, enthusiastic, joyful, communicative, talkative, enterprising, and experience positive feelings and excitement. However, employees with introvert (the other dimension of extroversion) personality are reserved, timid, distant, quiet, and preferred solitude life in the workplace life (Albladi and Weir2014; Henry et. al., 2018)

2.1.4. Agreeableness

Agreeableness contrasts a pro-social and communal orientation towards others with antagonism and includes traits such as altruism, tender-mindedness, trust, and modesty. An employee with an agreeableness personality is characterized by cooperative, sincere, and understanding, compassion, dependable, caring for others feeling, open-minded, valuing compromise than being skeptical, stubborn, competitive, and cautious in the workplace settings (Albladi and Weir, 2017; and Bansal, 2011).

2.1.5. Neuroticism

Employees with neuroticism personality tend to experience negative emotions such as anxious, nervousness, sad, tense, suspicious, worry, and constantly changing moods or feelings; needing the approvals of others, have, and being unreliable. Whereas, the opposite of neuroticism is called emotional stability characterized by being comfortable, confident, patient, open to criticism, resistant to stress, and other negative emotions (Eber and Ttsuoka, 2016).

Generally, recent studies have acknowledged the influence of personality or relatively enduring unique characteristics of an employee on InfoSec success, however, incorporating personality traits from executives' perspective into InfoSec management dimensions has largely been ignored (Pervin & John 2000; and Shropshire et. al., 2006).

For instance, a study by Barrick et. al. (2001) on five-factor personality and InfoSec management indicated the positive influence of personality (particularly conscientiousness and agreeableness) on InfoSec management. Also, emotional stability and openness negatively influenced the strategic InfoSec management component.

Similarly, at different times, different researchers came up with different findings. For example, Warrington (2017) found conscientiousness and agreeableness significantly related with and predict secured file protection behavior; whereas, openness to experience (e.g. the need to browse and search more information), extraversion (e.g. multiple relationships with others and easily persuaded behavior), and neuroticism (e.g. displaying tense and uncontrolled emotion) are associated with high InfoSec vulnerability behaviors.

Conversely, Witt et. al. (2016) found agreeableness positively linked with high InfoSec beaches, because being agreeable (having traits of helping and trusting with others) significantly predict high information and security password sharing behavior with others.

Fortunately, the information in the computer or printed document may lose its confidentiality, integrity, and availability.

Furthermore, recently personality constructs have been found to provide insights and explain even more variance in users' behaviors or practices related to InfoSec (Alavi, 2016). The finding by Albladi and Weir (2014) concluded that individuals with some traits of conscientiousness were found to be better in Infosec-related practices than other types. While, some other studies found traits of agreeableness than conscientiousness (Metalidoua et. al., 2014; Shropshire et. al., 2006).

2.2. Attitude

Attitude can be defined as a way of thinking, feeling, and behaving about something. It is also defined as a positive or negative evaluation of anything. It is a psychological tendency that is expressed by appraising a particular entity with some degree of favor, neutral, or disfavor Attitude comes from our beliefs, intension, and action (Fishbein and Ajzen, 1975).

An attitude demonstrates the feelings, behaviors, and thoughts of individuals about something. This feeling could be either positive or negative. Focusing on InfoSec, individual attitude demonstrates the internal feelings as well as the willingness of employees to obey or disobey properly behave or misbehave towards InfoSec policies, objectives, and even performance (Kaur and Mustafa 2013).

Attitude can be explicit or implicit; consciousness or unconsciousness of our belief and behavior (Muellerleile and Albarracin, 2016). Has emotional, cognitive, and behavioral components used for the formation of attitude in employees or any other persons. It can be formed as a result of personal experience, observation, and influence by social norms (Gundu, 2015). Employees with a positive attitude towards any situation (e.g., InfoSec) improve their performance easily. So, the development or formation of a positive attitude in one's life is helpful in facing any challenge (Safa et. al., 2015).

Even though employees' attitude is a well-known psychological factor to protect information and its systems, it is almost impossible to evaluate or forecast the impacts of their attitudes toward InfoSec. Because, the employees' behavior is assumed to be uncertain on different occasions such as the workplace, home, fieldwork, etc. (Harrison et. al., 2011).

Researchers such as Ahlan et. al., (2015) explained positive attitudes about InfoSec and their involvement in the information process is an important factor that impacts the InfoSec performance in an organization setting. Besides, Harrison, et. al., (2011) indicated attitude as the employee's favorable or unfavorable feelings towards organizational as well as organizational InfoSec policies, standards, and performances.

Also, research has shown that a user's experience and involvement influences their perceptions or attitudes about InfoSec. Also, Lapsley and Hill (2009) highlight the direct relationship between attitude and behavioral intent that make employees successful in their InfoSec issues. Furthermore, an employees' attitude towards workplace InfoSec policies compliance greatly affects their security behavior. When employees develop a positive attitude and participate in activities that are focused on a commitment to the organization's InfoSec goals and engage with like-minded colleagues in such matters, there is a positive effect on InfoSec performance (Pattinson et. al., 2015). Also, Parsons et al. (2014) noted favorable attitude towards information security positively correlated with the perceived as well as the actual performance of information confidentiality, integrity, and availability.

Employees' attitude is also influenced by InfoSec experience, awareness, performance (Ahlan et. al., 2015). Related to this, Kaur and Mustafa 2013) showed that once users perceive or have high InfoSec performance and experience in InfoSec threat, they are more likely to take protective actions.

In contradict, Michael (2016) suggested that having a positive or negative attitude towards InfoSec policies, practices, and cultures could not lead to negative or positive outcomes or information threat and harm or doesn't have an effect on employees InfoSec behaviors. While, technical knowledge, skills, experiences, and awareness of Information threat prevention matter a lot.

Researchers, managers, and users evaluate the InfoSec effectiveness of the individuals, most commonly used satisfaction measurements. As Pattinson et. al. (2015) noted that InfoSec satisfaction is equated to perceptions of easiness and usefulness of the information. Accordingly, the research shows this as a significant predictor of InfoSec effectiveness. With this, Maçada (2015) concluded that to understand employees' InfoSec effectiveness or performance using such security pleasure or displeasure measures can be risky because it will not give you sufficient data.

2.3. Perceived Information Security Performance

Prior to describing the concept of perceived information security performance, it's better to start with the concept of information security and performance. Information security (InfoSec) is the practice of protecting information by mitigating information risks. It involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, and modification (Kaur and Mustafa, 2013).

Similarly, Kruger, et. al. (2011) explained that InfoSec is a process that enables to protect of any physical (e.g. paperwork) and electronic (e.g. computer and email files, etc.) from unauthorized access, use, disclosure, harassment, modification, or destruction to provide confidentiality, integrity, and availability.

Information security performance referred to the behavioral engagement or actions of an employee to protect those electronic as well as non-electronic files, documents, and workplace information from unauthorized access using various InfoSec measures such as strong computer passwords, file shelf keys, etc. (Alavi, 2016). While, perceived InfoSec performance referred to the view that employees have towards their information security practices or behaviors include the use of passwords to make workplace information confidential and prevent it from unauthorized changes, deletion, adding, or modification (Bernik and Prislan, 2016).

Therefore, as Metalidoua et. al. (2014) and Joseph (2016) implied numerous technical advances in InfoSec sciences do not always produce more secure organizations. Information security in organizations cannot be understood as solely a technical problem. Since it's operated by employees, it has also a personality, attitude, and other psychological aspects

Usually, the personality difference and attitude are linked to one another and influence how employees view and interact with InfoSec behaviors. This interaction is often detrimental to InfoSec performance such as information confidentiality, integrity, and availability (Pattinson et. al., 2015); Henry et. al., 2018). Therefore, it is evident that solely technical solutions are unlikely to prevent information security breaches. Organizations need to instill and maintain positive attitudes and InfoSec sensitive personality traits in their employees (McCormac et. al., 2017).

In the same manner, as data, instructional files, documents, computers, and other digital devices become essential to business, commerce, and service delivery practice for all organizations,

they have increasingly become the target for information attacks. However, most organizations and employees believed that all the information in the device can be securely presented for the right time if they have employees with better technical skills and knowledge (Hinson, 2003)

However, Alhassana & Adjei-Quayeb (2017) explained that whether it's physical or electronic, every organization and/or employee has information that can be subjected to InfoSec issues. Thus, beyond the technical knowledge of information security, such organizations must consider the personality traits, attitude, and other psychological aspects of their employees, when measuring their InfoSec performances and take remedial measures to tackle their limitations. In this regard, Campbell et. al. (2010) implied that the employees with organized personality traits and positive attitudes towards InfoSec beaches have positive impacts on preventing and/or securing their workplace files at hand.

As a variety of researchers and literature such as Information Security Forum (2003); Koivisto and Ilvonen (2010); and Kruger and Kearney (2015) suggested InfoSec performance in the organization context includes balanced protection of any workplace information known as the CIA triads. *Confidentiality* (employees' ability to keep, control, protect, and secure the information from the unauthorized accessors or make it limited to the authorized users); *integrity* (employees ability to kept the information from unauthorized modification, intentional or unintentional change, insertion of incorrect information during storage, transmission, and usage, or kept it accurate and consistent unless authorized changes are made); and *availability* (employees ability to present every component of the information to the right users when needed and have sufficient backups). For example, organizations such as Amazon.com will require their servers to be available 24 hours a day, 7 days a week (Alavi, 2016; Ajay and Micah, 2014).

Similarly, in Ethiopia, banks, Automated Teller Machine (ATM), and other national security agencies like INSA's information and its systems must be available and properly function 24 hours a day (Information Security Risk Assessment Team/ISRAT, 2019).

Accordingly, Posthumus and Solms (2012) indicated that keeping these triads efficient can be varied as per the personality difference and attitude of the employees. For instance, Kruger and Kearney (2015) suggested that attitude can be explained by 68.9 %, 51.1 %, and 53.9 % of the variances in the employees' information confidentiality, integrity, and availability, respectively.

Moreover, personality differences, attitudes, and InfoSec behaviors of employees are reciprocally associated and predicted. For example, Jain and Pal (2017) found 29 % of employees InfoSec in the confidentiality dimension is predicted by the favorable attitude towards organizational InfoSec policy and compliance behavior, while 24 % of employees' attitudes are predicted by their InfoSec. Also, Mekovec and Hutinski (2015) indicated that 31 % of the variance in employees' InfoSec performance can be explained by conscientiousness (being having organized and decisive behavior).

Generally, even if the above empirical findings have shown the directional and reciprocal influence between employees' personality differences, attitude, and information security behaviors, they were not examined using the three InfoSec dimensions (CIA triads) together.

2.3.1. Extent of Employees Information Security Performance

Information security is not a single matter of Information Technology (IT), it's now a critical success factor for the whole organization. Because organization managers discovered that information is one of the most valuable assets like every physical asset that must be protected. To protect it from unauthorized users, they believed that their employees' performance on the InfoSec issue must be maximized (Tenney et. al., 2015).

According to the Computer Security Institute (2013), 1, 000, 000 InfoSec snatching trials are tried from China to different world organizations per year. Among this figure 22 % of InfoSec beaching incidents are successful. The success of the information confidentiality, integrity, and availability of beaching actors is due to the weak InfoSec performance of employees.

Also, the INSA's Computer Security Team/CST (2019) reported, 153 national computer InfoSec threats are attempted in a budget year and only 29% are correctly prevented. According to the International Organization for Standardization/ISO 31000 (2018), these statistics implied the low InfoSec performance of employees as well as organizations.

In this regard, Uffen et. al. (2013) argued, even if, there is a considerable amount of research literature on the interaction between general human behavior and computer InfoSec, there is very little rigorous research devoted to employee's personality and attitude difference that may influence the safe/unsafe employees behaviour related to their InfoSec performance. It has only been in the last decade that literature has emerged out of the InfoSec discipline that discusses the impact of individual behavior whilst using the information in the computer (Campbell et. al., 2010; and Shropshire et. al., 2006).

2.4. Variations in the InfoSec Performance of Employees' across Demographic Variables

According to Savola's (2015) suggestion, the length of employees' InfoSec training significantly relates to and predicts their InfoSec performance (in the information confidentiality dimension *(r = .58 and R^2 = .22)*. Further, he suggested that compared to older age groups and higher positions (e.g. managers), the late adolescents and early adults particularly those aged between 18 and 25 years old and lower-level positions (e.g. junior employees) are more susceptible to InfoSec vulnerability problems.

As compared to men, women are more susceptible to low InfoSec performance, because phishing emails study by Metalidoua et. al. (2014) and McCormac et. al. (2017) indicated that women are more responding to phishing emails which significantly affect their information confidentiality, integrity, and availability.

Moreover, regarding the habits of keeping any information confidential without any marginal change, deletion, or loss, Tenney et. al. (2015) found employees with male gender, older adults aged from 34 to 39, higher educational level, and work experience are less vulnerable to weak InfoSec performance problems than their counterparts.

2.5. Theoretical Orientation of the Study

The theoretical framework of this study was adapted from the Big Five Personality model of John & Srivastava (1999), and the Knowledge, Attitude, and Behavior (KAB) model of Kruger and Kearney (2006). The Big Five Personality model was developed for measuring the human aspects of information security performance using personality differences, while the KAB model was developed for measuring the information security awareness as well as performance using knowledge, attitude, and behaviour of individuals in an organization setting.

The Big Five personality model is used extensively to understand and predict numerous factors in diverse and complex environments. It is also the leading theoretical model for measuring and understanding personality in the five factors such as openness, conscientiousness, extraversion, agreeableness, and neuroticism (Shropshire et al., 2006). While, little research has been conducted to examine the relationship between personality and InfoSec performance, Pattinson et al. (2015) found fewer workplace information security accidents with employees

of conscientious personality traits and found higher information deletion or loss with employees of openness, extraversion, agreeableness, and neuroticism types.

On the other hand, the KAB model has been criticized by Harrison, et. al. (2011) for its small positive relationship between knowledge, attitude, behavior, and InfoSec aspects. However, Alavi (2016). indicated that the problem is not with the model itself, but how it is applied, the conceptualization of variables that a particular study is examining, how the model relates to other variables, and how they are measured are important issues that need to be considered.

Generally, as discussed above, the two models independently tried to indicate the direction of the relationship between personality difference, attitude, and information security. Accordingly, the present study was guided by mixing and adapting the Big Five Personality model and the KAB model. That means, the researcher took all the big five factors from the Big Five Personality model and attitude from the KAB model and constructed a single adapted model.

Moreover, the model showed the perceived InfoSec performance differences of employees as a function of their demographic characteristics such as sex, age, work experience, level of education, job position, and length of InfoSec training taken. Further, see figure 1 below.

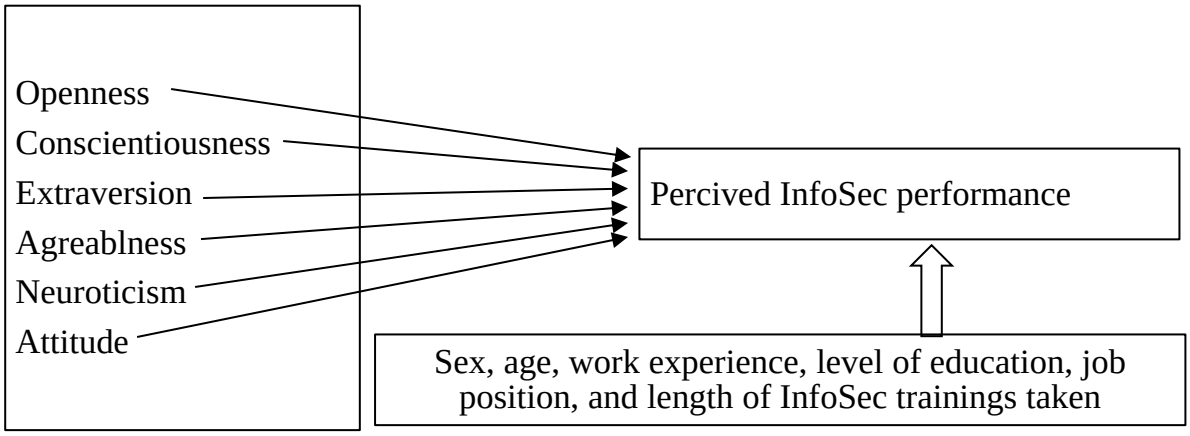

Figure 1: the conceptual framework of the present study

2.6. Summary

As the literature review has shown most of the time, conscientiousness, agreeableness, and a positive attitude towards InfoSec practice and policies are positively associated with the InfoSec performance of employees in an organization setting (particularly with the information confidentiality dimension).

Looking into the socio-demographic trends, the length of InfoSec training plays a significant role in predicting the InfoSec performance of employees. Women are more susceptible to InfoSec beaches particularly in the opening and clicking the phishing emails. The late adolescents and early adults particularly those aged between 18 and 25 years old are more susceptible to information security vulnerability problems compared to older age groups.

Generally, regarding the issue under study, inconsistent findings had been observed across researchers, time, place, other settings, or contexts. Therefore, this study aimed to test the issue under Ethiopian, particularly in the INSA context.

Chapter Three

Methods

3.1. Research Design

As the title of the study and its research questions directly inferred, this study employed a correlational research design. As Marczy et al. (2005) suggested a correlational research design is used to describe the statistical association and prediction between two or more variables. Therefore, in this study, the researcher has collected self-report data from participants and assessed the association between employees' personality differences, attitude towards InfoSec, and perceived InfoSec performance in the INSA context.

Beyond examining the nature and extent of the relationship between the study variables, the researcher has also predicted the variability in employees' InfoSec performance as accounted by their personality difference and attitude.

3.2. Study Site

This study was conducted in Information Network Security Agency (INSA). Two basic rationales were presented behind selecting this study site.

The first rationale was since INSA is a nationally responsible agency that vastly works on the issue of information security, the researcher assumed it as highly concerned and familiar with the issue understudied. Also, to the researcher long-lived experience and observation, there was lack of compressive empirical data used to design a context-based information security policies, standards, and frameworks which integrates the issue of employees' personality difference and attitude. The context-based empirical data will help to maintain an appropriate InfoSec culture and practice in the agency.

Second, the agency has long-lived experience in creating InfoSec awareness, preventing InfoSec risks, and improving the InfoSec performance of employees in and outside of the agency. In doing these activities, the agency was focusing on the technical and technological skills of the users rather than incorporating their personality difference, attitude, and other psychological factors (Information Security Risk Assessment Team/ISRA, 2019).

Geographically, INSA is found in the capital city of Ethiopia known as Addis Ababa, Lafto Sub-city (District 04) around St. Gabriel Church. The agency was first established in Proclamation No 130/2006 or re-established in 808/2013 by the council of Ethiopian Federal Democratic Peoples Representatives. Its establishment aimed to keep the country from any InfoSec attacks and achieve an optimum InfoSec performance of its organizations as well as users or employees (Federal Negarit Newspaper, 20th year, No.6, 2014).

Currently, INSA has a total of 1,067 staff members (male = 705 & female = 362) functioning in the four different directorates such as Aerospace, Engineering Solution and Research, Cyber Security, and Assurance directorates. Employees in all directorates were working towards maintaining and ensuring the InfoSec performance of the country in a variety of perspectives and job positions.

3.3. Data Source or Target Population

The data source or target population of this study was all the current (2020 G.C) employees of INSA. The total number of employees' in the current year were 1,067 (male = 705 & female = 362). But, janitors, child day careers, and gate security staff were not included in this study. The rationale behind to exclude these staff members were: First, these staff members were not full-time workers, they were constantly changing even within an hour, and cannot be constantly available in and around the office, as a result, the researcher assumed it will be difficult to collect sufficient data from them. Second, the researcher assumed these staff members have little exposure to the organization and computer-based InfoSec issues.

3.4. Samples and Sampling Techniques

The participants of this study were the ordinary employees, supervisors, team leaders, and directors who have adequate experience on the issue of InfoSec practices or traditions in organizational contexts.

The four major reasons were presented to focus on these groups of research participants. First, from its establishment the prime aim of the agency was to ensure the InfoSec performance of the state as well as the individuals. Therefore, the staff in this agency were assumed to have better exposures, experiences about InfoSec related issues, and will give valid data about the issue under study. Second, related to the first, the employees in the agency have a long-lived experience in training and sharing experiences about InfoSec issues to other national

organizations. Third, without sufficient context-based empirical data, the agency works hard on minimizing organizational InfoSec vulnerability issues that can occur due to employees' personality and attitudinal factors. Therefore, since the researcher himself was part of the staff in the agency, he was highly interested to assess the variables under study and provide valid and context-based empirical data for better practice.

With the issue of sampling, a stratified random sampling technique was employed. Taherdoost (2016) and Alvi (2016) suggested a stratified random sampling method used when the target population is heterogeneous. Based on this suggestion, the researcher has preferred these sampling techniques because the population of INSA was diversified in a variety of ways such as directorates they worked on, sex, age, work experience, educational level, job position, and length of InfoSec training taken. Therefore, the method helped the researcher to select a representative sample as it captures the diversity of the participants and makes a generalizable conclusion to the study population.

3.4.1. Sample Size Determination Procedure

Employees in the agency were categorized or stratified based on the five already existed major strata (taking directors as a 5^{th} stratum). Based on job position (ordinary employees, supervisors, and team leaders), every four strata were further categorized into sub-strata gave 12 sub-strata (12*3 job position levels). Then, based on sex, these sub-strata further categorized and gave 24 strata, by adding the 5^{th} strata, the total strata of this study were 25.

Considering the strata and size of the population in each stratum, the proportional research participants were determined using Yemane's (1967) simplified proportional sample size determination formula. Because, Yamane's formula provided a relatively more accurate sample size than the sample size determination table and online sample size calculator like Rao soft (Ajay and Micah, 2014). Therefore, the sample size determination formula of the current study with 95% of confidence interval and with 5% acceptable sampling error or 0.5 level of precision was presented as follows:

$$n = \frac{N}{1 + N(e)^2}$$

Where n represented sample size, N represented population size, and e represented sampling error (level of precision).

Even though, proportional sampling technique employed to determine the proportional sample size with respect to their population size, the sampling was generally disproportional. Because the samples taken from each stratum was varied. Generally, the sample size of this research was 291. However, considering Endrias (2019) and Taherdoost (2017) suggestion that 10 % added for non-response items and non-returnable questionnaires, the total sample size was approximately 320.

To determine the proportional sample size in each stratum, the researcher was used the formula below:

$$\mathrm{nh} = \frac{\mathrm{Nh}}{\mathrm{N}} \times n$$

Where nh represented proportional sample size in the h stratum, Nh represented total population size in the h stratum, N represented the total population size (1,067), and n represents the total sample size (320). Table 1 below further illustrated the population, sample size, and sampling procedure that was drawn from each stratum.

Table 1: Sample size drawn based on the strata

Categories / Directorates	**Specific strata**	**N (total population)**			**n (sample size drawn)**		
		Female	Male	Total	Female	Male	Total
Aerospace	Ordinary expert	61	141	202	19	42	61
	Supervisors	10	14	24	3	4	7
	Team leaders	4	9	13	1	3	4
	Total			**239**			**72**
Engineering Solution and Research	Ordinary expert	97	175	272	29	52	81
	Supervisors	9	19	28	3	6	9
	Team leaders	3	11	14	1	3	4
	Total			**314**			**94**
Cyber Security	Ordinary expert	89	149	238	27	44	71
	Supervisors	3	11	14	1	3	4
	Team leaders	2	7	9	1	2	3
	Total			**261**			**78**
Assurance	Ordinary expert	74	148	222	22	44	66
	Supervisors	3	9	12	1	3	4
	Team leaders	2	4	6	1	1	2
	Total			**240**			**72**
Agency directors as a stratum	**Total**	5	8	**13**	1	3	**4**
	Grand Total	362	705	**1067**	110	210	**320**

Note: - the term directorate referred to the job department in which in charge of a particular dimension of work in the agency

3.4.2. Sample Selection Procedure

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. Meaning, 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 (in the morning, before they start their job or 8:00 AM to 9:30 AM). Then, they provided oral orientation about the objectives of the study to the whole staff in their office and asked their consents.

Finally, by counting the number of employees who were willing to participate in the study, they randomly provided or 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.

3.5. Measures

3.5.1. Instrument Development Procedure

Except for the demographic measures, all the scales used in this study were Likert type self-reported questionnaires. Generally, the questionnaire has three major sections. These were: the demographic measures, five-factor personality, attitude, and information security performance measures. More specifically: -

I. Participants' demographic data: - the participants' demographic data was the first section of the data collection instrument that consisted of questions about participants' sex, age, work experience, educational level, job position, and length of InfoSec training taken.

II. Big Five-Factor Personality Inventory: - the five-factor personality inventory was adapted from the John and Srivastava (1999) Big Five-Factor Inventory (BFFI) and used to measure the personality differences of employees.

The BFFI has 5 sub-scales namely, openness, conscientiousness, extraversion, agreeableness, and neuroticism. Each sub-scale has 6 Likert type-specific items with both positively and negatively worded. Sample items include: I make plans and follow through them (from the positively worded) and I often forget to put things back in their proper place (from the negatively worded). Employees' responded to each item on a 4-point scale ranging from 1 (strongly disagree) to 4 (strongly agree).

The researcher presented three salient advantages in choosing BFFI over other instruments. First, the BFFI was the widely used and applicable instrument in measuring employee's personality differences in the areas of InfoSec issues with showing consistently high convergent validity with other self-report scales and peer ratings of the Big Five measures (John and Srivastava, 1999).

Second, it has inherent generalizability significance in its systematic and comprehensive approach to personality (Metalidoua et. al., 2014). The factors don't mean representing a specific theoretical perspective, but rather a complete taxonomy of terms that allowed employees to describe themselves and others (Alavi, 2016). This generalizability permitted the use of the model across many research areas, including InfoSec related issues.

The third advantage of choosing this scale was that the behavioral patterns associated with the factors were well known in comparison to a large number of specific factors (Pervin & John 2000). For example, numerous organizational studies have identified a significant inverse relationship between information security risk involvement and conscientiousness personality factor (John & Srivastava, 1999). Meaning, individuals who rated themselves as thinking before acting, following norms and rules, and planning and organizing tasks were less likely to be involved in InfoSec related risky activities than those who rated themselves as lower on the same attributes (Shropshire et. al., 2006).

Lastly, the BFI with its sub-scales has a high Cronbach alpha value across organizations, various translations, and different population (Hadlington, 2017). For instance, in various studies the average alpha value of openness =.81, conscientiousness = .86, extraversion = .83, agreeableness = .89, neuroticism = .87, and overall Cronbach Alpha value = .85 (Alavi, 2016; John & Srivastava, 1999; & Metalidoua et. al., 2014).

III. Attitude: - the attitude scale was adapted from the Attitude towards the InfoSec Scale (AISS). AISS was designed to measure human attitude towards information security in particular to organization settings by Ahlan et. al. (2015). The AISS has 15 Likert type items with both positively and negatively worded items. Sample items include: I worry about the information being exposed (from the positively worded) and Information security issues should not be a priority within the agency (from the negatively worded). Employees' responded to each item on a 4-point scale ranging from 1 (strongly disagree) to 4 (strongly agree).

Due to the following prior reasons, the researcher has preferred AISS. First, AISS developed based on the comprehensive measure of attitude towards an information security perspective. Second, it was designed to examine employees' attitudes towards InfoSec in particular to organization settings. Third, it has a high (≥ .86) Cronbach Alpha value across organizations and various language translations (Hadlington, 2017).

IV. Perceived Information Security Performance Scale: - the perceived information security performance scale was adapted from the Pattinson and Anderson (2007) perceived InfoSec Performance Scale (ISPS) and used to measure the information security performance of employees in the CIA triads.

The ISPS is composed of 18 items measuring the compressive InfoSec performance on a 4-point Likert-type scale ranging from 1 (strongly disagree) to 4 (strongly agree). The items were worded both positively and negatively. Sampled items include: I use multiple security control procedures (e.g., locking passwords) to prevent unauthorized information creation, alternation, change, add, and deletion (from the positively worded), and I did not check and evaluate the integrity of information in my computer (from the negatively worded). Employees' responded to each item on a 4-point scale ranging from 1 (strongly disagree) to 4 (strongly agree).

The rationales behind preferring this scale were: First, the scale developed based on the International Organization for Standardization (ISO) 31000 (2018) for users and organizations InfoSec related performance measure specifications. Second, it included all three InfoSec domains i.e. confidentiality, integrity, and availability (CIA) triads (Uffen et. al., 2013). Third, the scale developed in line with the 10 by 10 metrics of InfoSec performance measure, as a result, it helps to measure the compressive and an optimum level of both physical and electronic InfoSec performance of the employees in an organizational setting. Fourth, the scale was developed to measure the staff's perception of their information security performance in organizations (Hinson, 2003).

Moreover, its reliability in previous studies found between Cronbach alpha .79 to .86 which indicated high reliability (Macada, 2015).

3.5.2. Validation Procedure

To obtain valid and reliable data, instruments must have highly established content validity and psychometric characteristics (Zelt et. al., 2018). Based on this assumption, content validity was established for a total of 63 translated questionnaire items.

A panel of 10 subject matter experts were purposively identified (5 from social psychology and 5 from information system security fields). The identification process was based on their expertise, qualification, and experiences. Therefore, the panelists were high-level expertise, master's degree holders, and have a minimum of 7 years of work experience in the Information Network Security Agency office.

A draft of hard copy data collection instruments was given to the 10 panelists by hands and orally briefed about how to judge the adequacy, appropriateness, and non-ambiguity or clarity of each item and directions of the instruments.

Accordingly, Lewashe's (1975) quantitative approach content validity technique that involved the statistical validity estimation ratio was employed. Because the statistical content validity ratio (CVR) is a useful technique to reject a specific non-essential item from the initial item pools 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 of CVR expressed as:

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

Where ne refers to the number of panelists pointing the item 'essential' and N refers to the total number of panelists.

The value of CVR ranges between -1 to +1. The positive value indicated the item is appropriate, clear, or; the negative value indicated the item should be reworded, changed, or rejected; and the value of .00 indicated that 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 assumed to be 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)*. As Lewashe (1975) suggested, *'essential'* items best represent good content validity.

Furthermore, based on a one-tailed test and α=.05 significance level, Lawshe's has established a decision rule on the value of CVR with varying panel sizes. Table 2 below illustrates this;

Table 2: 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
15	.49
20	.42
25	.37

Source: *Lawshe's (1975) minimum CVR value determination for the varying number of panelists*

As the decision rule implied, only the items which meet the minimum CVR value will be retained, while the remaining will be removed. Based on this assumption, a total of 63 questionnaire items were given to 10 subject matter experts with clear instructions about the purpose of the study instruments and the way they will rate each item.

3.5.3. Results of Validation

The researcher obtained the response items from panelists and counted the number indicated as *'essential'* for each item. Then, the content validity ratio of each item was computed using Lawshe's formula. So, based on the decision rule *(see table 2 above),* the items having a CVR value of <.62 were rejected and the items having a CVR value of ≥ .62 were accepted.

Finally, two items (one from the openness sub-scale and the other one from the extraversion sub-scale) identified as having a CVR value of less than .62, while the rest, which recorded greater than .62 retained and used for the pilot study. Besides, the content validity index (CVI) computed for items retained in the scale was 89%. Regarding this, Zelt et. al. (2018) suggested that the instruments were viewed as valid and acceptable, and therefore used as assessment tools.

3.5.4. Translation Procedure

All the data collection instruments used in this study were originally developed in the English language, and translated into the Amharic language. Because, literature e.g. Raudenbush (2015), suggested translating the data collection instrument from the source language to the target language brings high context validity; significantly improved the reliability and validity of the instrument, the data, and even the findings of the study. Similarly, Dhamani and Richter (2011) suggested, translating the data collection instrument from its originally developed language to the target language makes the participants feel comfortable and helps the researcher to obtain high response quality. It also helps the researcher to determine the appropriateness, relevance, quality, adequacy, and wording of items in a data collection tool.

Generally, the educational level of the pilot study participants who completed the self-report questionnaires was ranged from diploma to 2nd-degree level. But, by considering the literature suggestions above and make the participants feel safe, understand items better, and provide their response properly, the scales were translated from the English language to Amharic (the official working language of the participants) by the subject matter experts. Also, to ensure the equivalence of items translated into Amharic and developed in its original English language, the back-translation practice has been made.

Accordingly, Dhamani and Richter (2011) suggested 3-9 subject matter instrument translation experts will be enough for students' theses at the master's degree level. Therefore, a total of 4 subject matter experts participated in both forward and backward translation practices.

One expert was made the forward translation and the other one expert was made the backward translation. Both of them were English language literature lecturers in Wolkite University and have master's graduate degree, knowledge, and experience of the language in which the instrument originally developed and translation to be made. Besides, they were fluent Amharic language speakers.

Finally, the two subject matter experts (one social psychologist and the other one information system security graduate) were come together, edited, ensured the equivalence of the Amharic and English versions of the instruments, and approved it for a pilot study. Both of them were experienced experts in the areas of human behavior and information security risk assessments in the Ministry of Peace Office and INSA respectively.

As a result, the social psychology expert was treated issues related to the clarity, validity, and professionally of terms or wording of items to the suitability of participants' context; also, the information system security expert was treated issues related to the validity, clarity, suitability of terminologies, and wordings to the context of the participants.

3.5.5. Scoring Procedure

I. Demographic data: - the participants' demographic data had collected using 6 questions. Accordingly, the participants' sex such as males scored as 1, and female scored 2. The age and work experience of participants was scored as it is. Participants' educational level: diploma scored as 1, first degree scored as 2, and second degree scored as 3. The participants' job position: ordinary expert or employee scored as 1, supervisor scored as 2, team leader scored as 3, and director scored as 4. Lastly, the length of InfoSec training taken by the participants: 2 days (16 hours) scored as 1, three days (24 hours) scored as 2, and 5 days (39 hours) scored as 3.

II. The Big Five-Factor Personality Inventory: - The five-factor personality scale has 5 sub-scales: openness, conscientiousness, extraversion, agreeableness, and neuroticism. Each item in each subscale 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 in the instrument were reversely worded. Accordingly, for the positively worded items, strongly disagree was scored as 1, disagree was scored as 2, agree was scored as 3, and strongly agree was scored as 4. In contrast, for items that were negatively worded, strongly disagree was scored as 4, disagree was scored as 3, agree was scored as 2, and strongly agree was scored as 1.

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. Then, the higher the scores in each sub-scale implied the dominant openness, conscientiousness, and extraversion, agreeableness, and neuroticism personality characteristics in the five-factor personality measure.

III. Attitude Scale: - The attitude scale has a total of 15 items rated on a 4-point Likert scale ranging from 1 (strongly disagree) to 4 (strongly agree). To avoid some possible response biases, some items in the instrument were reversely worded. Accordingly, for the positively worded items, strongly disagree was scored as 1, disagree was scored as 2, agree was scored

as 3, and strongly agree was scored as 4. Contrarily, for items worded negatively, strongly disagree was scored as 4, disagree was scored as 3, agree was scored as 2, and strongly agree was scored as 1.

With reversely coding the negatively worded items, the total raw score for a total of 15 items yielded from 15 to 60. Last, the higher the score indicated a favorable attitude towards information security, the lower the score indicated an unfavorable attitude towards information security, and the mid-point between 30 to 34 indicated neutrality.

IV. Perceived Information Security Performance Scale: - The perceived information security performance scale has a total of 18 items rated on a 4-point Likert-type scale ranging from 1 (strongly disagree) to 4 (strongly agree). Like personality and attitude scales, some items in the instrument were reversely worded. Accordingly, for the positively worded items, strongly disagree was scored as 1, disagree scored as 2, agree was scored as 3, and strongly agree was scored as 4. Similarly, for items worded negatively, strongly disagree was scored as 4, disagree was scored as 3, agree was scored as 2, and strongly agree was scored as 1.

Following reversely coding the negatively worded items, the total raw score of the 18 items yielded from 18 to 72 in which the higher scores indicated the higher perceived InfoSec performance, the lower scores indicated lower perceived InfoSec performance of employees, and the score laid down between $\geq$ 34 to $\leq$ 40 taken as moderate information security performance score.

3.6. Pilot Testing

3.6.1 The Purpose of Pilot Testing

Beyond validating the data collection instruments by the subject matter experts, the researcher has also conducted a pilot study on a sample of 50 representative participants. The rationale to conduct a pilot test was to test the practicality of the instruments particular to the INSA context, as a result, it helps the researcher to identify the defects, improve them, and help to establish contextual reliability of the scales. Accordingly, Schattner and Mazza (2015) suggested that beyond establishing the reliability of the scales, pilot testing allows the researcher to ensure the adequacy of the item's wording, length, instruction, and help to determine the initial response rate of the items.

Before administering the data, collection instruments, the intention of the pilot and main study was described to the participants and verbal consent from each participant has taken. The researcher himself handled every practice of the pilot study.

3.6.2. Characteristics of Pilot Test Participants

Schattner and Mazza (2015) suggested ≥ 30 pilot study participants are enough in the case of quantitative study. Besides, the researcher advisor (Dr. Dame) suggested 50 to 70 participants for establishing good instrument reliability and response rate. Therefore, keeping both suggestions into consideration, the researcher randomly sampled 50 employees of the Cyber Defence and Operation department office, which represented almost similar characteristics to the main study samples.

The department office was found a little bit distant from the main office and purposively excluded in the main study. A suggested by Taherdoost (2017), the proportional sample size was taken using $Np \times \frac{n}{N}$ formula. Where Np referred to the total sample size of the study indicated female (110) or male (210), n referred to the total sample size of the pilot study (50) and N represented the total sample size of the study (320).

Based on this formula, 17 female participants and 33 male participants were randomly selected in their working office and participated *(See table 3 below for details).*

Table 3: Demographic data of pilot study participants

Variable	Label	Figure	Percent
Sex	Female	17	34 %
	Male	33	66 %
Age	Minimum	27 years old	-
	Maximum	36 years old	-
	Average	30 years old	-
Level of education	Diploma	5	10 %
	First degree	37	74 %
	Second degree	8	16 %
Work experience	Minimum	2 years	-
	Maximum	10 years	-
	Average	5 years	-
Job position	Ordinary expert	35	70 %
	Supervisor	11	22 %
	Team leader	4	8 %
Length of InfoSec training taken	Minimum	3 days	-
	Average	5 days/one week	-
	Maximum	6 months	-
	Total N	50	100 %

Source: Pilot study data

3.6.3. The Procedures and Results of Reliability Indices

The reliability of each data collection scale was established using Cronbach Alpha (α). Because, in different psychological researches, Cronbach alpha computation has taken as the best indicator of the internal consistency of items with the Likert type scales (Teijlingen and Hundley, 2014).

Regarding the Cronbach alpha coefficient interpretation, Teijlingen and Hundley (2014) suggested the following rule of thumbs: if $\alpha \geq .9$ is excellent, $.8 \leq \alpha \leq .89$ is good, $.7 \leq \alpha \leq .79$ is acceptable, $.6 \leq \alpha \leq .69$ is questionable, $.5 \leq \alpha \leq .59$ is poor, and $\alpha \leq .5$ is unacceptable. However, in most cases, Cronbach alpha of $\geq .70$ was considered a good indicator of scale reliability (Zelt et. al., 2018).

The Cronbach alpha index was computed in the SPSS package (version 25). First, the data were collected from the pilot study participants and feed into the software package; then the reliability coefficient index was computed for each scale and sub-scale. Accordingly, the Cronbach alpha reliability coefficient of each scale calculated as: .81 for BFFI *(.90 for openness sub-scale, .87 conscientiousness sub-scale, .91 extraversion sub-scale, .84 agreeableness sub-scale, and .75 neuroticism sub-scale*); .83 for HAIS, and .89 for ISPS. Furthermore, table 4 below illustrated the item-analysis output for the multi-item scales of the big five-factor personality, attitude, and InfoSec performance measures.

Table 4: Statistical outputs of Cronbach alpha for the pilot study

Description	BFFPI sub-scales							
	O	C	E	A	N	BFFPI total	AIS	ISPS
Number of items	5	6	5	6	6	28	15	18
Reliability	.90	.87	.91	.84	.75	.81	.83	.89

Where, OCEAN referred Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism sub-scales respectively; BFFI- Big Five-Factor Inventory; AISS- Attitude towards Information Security Scale; and ISPS- Information Security Performance Scale

To be a scale reliable, all items must be positively correlated with the item total score within it. Deleting items having a weak and negative item-total correlation can significantly increase the Cronbach Alpha coefficient of the scale (Alhassana & Adjei-Quayeb, 2017).

Based on this, the researcher deleted some items which were not sufficient to meet the literature suggestion above. Accordingly, one item of the neuroticism sub-scale and the other one item of the ISPS was deleted for their context irrelevancy and negative item-total correlation output *(-.057, and -.062)* respectively. Except for those items deleted, the item-total correlation of all

the remaining items were above .77, which indicated a high item-total correlation value as Albladi & Weir (2014) suggested.

Generally, a total of 2 items were removed for their negative item-total correlation characteristics. Avoiding them can be brought a significant advantage in increasing the value of the Cronbach Alpha coefficient and improving the reliability of remaining items in measuring the study variables.

Table 5: Statistical summary of Cronbach alpha outputs for the main study

Description	BFFPI sub-scales							
	O	C	E	A	N	BFFPI total	AIS	ISPS
Number of items	5	6	5	6	5	27	15	17
Reliability	.91	.88	.93	.87	.90	.91	.89	.94

Where, OCEAN referred Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism sub-scales respectively; BFFI- Big Five-Factor Inventory; AISS- Attitude towards Information Security Scale; and ISPS- Information Security Performance Scale

3.6.4. Implications of the Pilot Study for the Main Study

From the practice of pilot testing such as instrument validation, administration, and results of the pilot test data, the researcher took the following significant insights used for input for the main study. First, the scales are viewed and taken as a valid and reliable tool for conducting the main study. Because any instructional and item ambiguity and non-response item effects have not been observed. Second, the item-total correlation analysis results suggested that the items in each scale have adequate internal consistency. This adequate internal consistency can confidently support instruments to collect data for the main study. Third, the pilot data analysis helped to test the assumptions of model statistical instruments used for the main study data analysis. Fourth, it significantly oriented the data enumerators to properly understand the backgrounds of the respective participants before instrument administration and data collection for the main study.

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.

3.7. Data Collection Procedure

Before data collection for the main study, the researcher purposively recruited the five data enumerators and familiarized them with the data collection instruments, items, and instructions. The rationales behind recruiting these data enumerators were: First, they have ≥ 3 years of work experience in information security research, data collection, and analysis activities across different governmental organizations in Ethiopia. Second, due to their convenience to the researcher, they assumed to be there during the data collection time. Finally, the researcher assumed the five data enumerators to be enough for the five major strata (one enumerator per major stratum). Except the one, the remaining four enumerators were managed 24 specific sub-strata under their major strata (6 specific strata per enumerator).

Following data enumerators recruitment, the researcher trained the data enumerators on how to approach participants (e.g. ethical greetings, communications, and self-introduction), describe the purpose of the study, take their consents, administer the questionnaire by hands, resolve confusions that can be raised when the participants respond to each item and collect the questionnaire back from the participants. Considering their experience, knowledge, and exposure to the data collection practices, the researcher planned and delivered 2 hours of practical training sessions at the conference room of the Agency.

The trained enumerators were sent to the assigned stratum with the desired number of duplicated instruments. The first half page of each instrument was contained an additional written explanation about the educational background and institutional affiliation of the researcher and the purpose of the study.

In each data collection office, the data enumerators organized the participants and read an oral message note about the nature and purpose of the study in which the results would be used. Then the data enumerators were provided with an adequate oral orientation on how to respond to items and administered questionnaires by their hands for those who gave their oral consent to fill the questionnaire. In order not to interrupt them from their work and assuming to get consistent responses in all participants, all the tools were administered before the participants started their regular tasks in their office (from 8:00 to 9:30 AM).

The majority of the filled instruments were collected in each secretary's offices of the participants. On the next day of the questionnaire administration, the data enumerators counted the collected questionnaires from each secretary's office and directly collected the remained questionnaires from the participants.

However, during the data collection time, the researcher has faced three major challenges. Following the provision of COVID-19 prevention and controlling proclamation No. 30/2013 by the Ministry of Health (MOH), most employees were not fully available in their offices. Due to this, the questionnaires were not fully administered as planned. Second, during the data collection time, the agency was shifting its working place from Bisrat Gebrel to Wollo Sefer. As a result, the employees were busy to take time and fill the questionnaire properly. The final challenge was the non-response rate (e.g. items jumping, missing, etc.).

Even though, the researcher faced with those problems, he took a long time and get the desired number of participants for the study, used the mean replacement method for missing values, and omitted 24 questionnaires which were useless or incomplete.

Generally, to ensure the accurate administration of instruments, data collections, elaborate instrument purposes, and clarifying ambiguities, doubts, and questions raised by the participants, the researcher was personally available with the data enumerators and successfully monitored all the data collection practices.

Furthermore, assuming the current state of coronavirus pandemics, every data collection practice was performed with respecting the anti-corona virus dissemination proclamation of the Ministry of Health and Ethiopian Community Health Institute. Accordingly, the data enumerators have used face masks, sanitizers before administering, and after collecting each questionnaire.

3.8. Data Analysis Procedures

The Statistical Package for the Social Science (SPSS) version 25.0. was performed to analyze the data collected from participants. Generally, a descriptive statistic such as frequency and percentage (for its appropriate nature with categorical level data); and the independent t-test, one-way ANOVA, Pearson Product Moment Correlation Coefficient Matrix, and hierarchical multiple regression data analysis techniques were employed for their appropriate nature with interval or ratio level data (Schattner and Mazza, 2015).

The descriptive statistics were used to assess the distributions of participants' socio-demographic characteristics such as sex, age, level of education, job position, length of InfoSec training taken by employees. Besides, it was used to describe the employees perceived InfoSec performance level in the INSA context.

Since, sex has only two levels, an independent t-test was employed to assess the research question that does the perceived InfoSec performance of employees in INSA vary as a function of sex? With an independent t-test, the data (scores) are independent of each other (assumption of independence), the test or dependent variable is normally distributed within two populations (assumption of normality), and the variance of the test variable in the two populations are equal (assumption of homogeneity of variance) were considered and satisfied.

On the other hand, since, level of education, job position, and length of InfoSec training taken have >2 already existed levels, one-way ANOVA was used to investigate the research question that does the perceived InfoSec performance of employees in INSA vary as a function of employees' level education, job position, and length of InfoSec training taken? Also, the assumption of the population in which the samples were taken are normally distributed, homogeneity of variance, and random sampling was fulfilled.

Also, the Pearson Product Moment Correlation Coefficient Matrix was employed to answer the research question that do age, work experience, personality difference, and attitude significantly related to the perceived InfoSec performance of employees' in the INSA context? Regarding this, Marczy et al. (2005) and Raudenbush (2015) suggested, Pearson Product Moment Correlation Coefficient data analysis technique is used, when the researcher is interested to assess the relationship between two or more variables.

Finally, hierarchical multiple regression analysis techniques were used to examine the research question that do personality difference, and attitude predicted (separately and jointly) the perceived InfoSec performance of employees in the INSA context? Regarding this, Raudenbush (2015) suggested that hierarchical multiple regression analysis techniques allow the researcher to control the effect of confounding variables and test the independent or joint contribution of the predictor variables to the dependent variable.

The Scheffe post hoc test, for its usefulness to considering unequal sample size between groups (Teijlingen and Hundley, 2014), the researcher was used to identify which mean significantly differs from the other in all significant F values of the univariate analysis. The statistical

significance level of the study was set at alpha .05. Also, the model assumption of normality, linearity, and homogeneity of variances was performed in all inferential statistical procedures.

3.8.1. Data Screening and Test of Model Assumptions

Before conducting the actual data analysis, the data were screened to check whether data entered correctly or not, missing values and determine on how to deal with those missing values, extreme values and determine on how to deal with those outliers, and the normality of the data and non-normality (Schattner and Mazza 2015; Zelt et. al., 2018).

Therefore, frequency counting was employed to check the accuracy of data entry and some extreme value cases in the data were eliminated to minimize their influence and made the data appropriate for the analysis. Also, the researcher dropped out of 24 questionnaires since they were almost incomplete and very difficult to treat.

Moreover, as Dame (2014) suggested, before deciding on whether to use parametric tests or non-parametric tests to analyze quantitative data, the assumptions of normality, linearity, homogeneity of variance, and multicollinearity must be tested.

Accordingly, first, the assumption of normality was tested using histogram and skewness tests, resulted in the means were nearly equal and the skewness was within the range of acceptance level (-1 to +1) for all scales and sub-scales, suggested that the data was reasonably normal and the assumption of normality was satisfied (Bernik and Prislan, 2016).

Second, the scatter plot analysis and statistical significance of the correlation coefficients between the IVs and DV tests were used to examine the assumptions of linearity and resulted in a significant F value of the ANOVA table and correlation coefficients ($r_{xy} > .30$) between IVs and DVs implied there was a good model fit or non-multicollinearity effect (Teijlingen and Hundley, 2014).

Lastly, the assumption of homogeneity of variance was tested using Levene's test and resulted that the values of the test statistic were found non-significant (> .05), indicating that the assumption of the equality of variances is satisfied for those scales and subscales.

3.9. Ethical Considerations

Taking the written of each participant was assumed to be costly by the researcher, the researcher with the data enumerators read the consent asking form and received each

participant consent verbally *(see appendix 3).* Accordingly, only those participants who gave their free consent to participate in the study completed a questionnaire package.

Following an important discussion about the overall aim and purpose of the study; the type of the data collection tools that will be administered and its procedures, the director checked and approved the unharmful effects of the data collection tools on the participants as well as the agency.

Also, assuming to get genuine responses, the participants were assured that their responses will be kept confidential and used only for research purposes.

Moreover, participants were informed that they have the right to stop filling the questionnaire at any point in time if they could not feel free and uncomfortable.

Chapter Four

Results

The major objective of this study was to assess the relationship between the personality difference, attitude, and perceived information security performance of employees in the INSA context. Accordingly, the following research questions were formulated by the researcher.

RQ1. What is the level of employees' perceived InfoSec performance in Ethiopia, INSA context?

RQ2. Does the perceived InfoSec performance of employees vary as a function of their sex, level of education, job position, and length of InfoSec training taken in Ethiopia, INSA context?

RQ3. Do age, work experience, personality differences and attitudes significantly relate to the perceived InfoSec performance of employees in Ethiopia, INSA context?

RQ4. Do personality differences and attitudes significantly predict the perceived InfoSec performance of employees in Ethiopia, INSA context?

Generally, the results of the study were organized and presented with the sequence of the research questions. Except for demographic data measures, all of the scales yielded interval or ratio level data. As a result, statistical techniques such as Independent t-test, one-way ANOVA, Person Product Moment Correlation Coefficient, and multiple regression were used to analyze the data.

4.1. Summary of Descriptive Statistics

4.1.1. Demographic Characteristics of the Employees'

Table 7: The demographic characteristics of the 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 %
	First degree	218	73.65 %
	Second degree	52	17.57 %
Work experience	Minimum	2years	-
	Maximum	10 years	-
	Average	6 years	-
Job position	Ordinary expert	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 7 above showed the demographic data of participants of the study who were able to fill the questionnaire. Based on the population size of the agency and implication of the pilot data in the previous sections, reasonably representative participants were sampled in sex, age, level of education, work experience, job position, and length of information security training taken categories. Accordingly, the data simply confirmed that the researcher can draw inferences about the target population (INSA employees) using the sample characteristics.

4.1.2. Distribution of Employees' Personality Difference

Table 8: Mean and standard deviation statistics of employees' personality difference

Personality Difference	**Mean**	**St. deviation**
Openness	13.87	2.91
Conscientiousness	15.15	3.01
Extraversion	12.53	2.95
Agreeableness	13.15	3.11
Neuroticism	11.01	2.71

Source: Questionnaire data, 2020

As table 8 above indicated that employees of INSA scored higher on the conscientiousness sub-scale *(M=15.15, SD = 3.01)* than openness *(M= 13.87, SD = 2.91)*, agreeableness *(M=13.15, SD= 3.11)*, extraversion *(M=12.53, SD= 2.95)*, and Neuroticism *(M=11.01, SD=2.71)* respectively. This implied that employees are more prepared, organized, disciplined, and avoid mess of files and documents that may lead to InfoSec performance problems than being open, sympathetic, quick, and emotionally disturbed to loss the confidentiality, integrity, and availability of information in their hands.

4.1.3. Distribution of Employees' Attitude towards InfoSec

Table 9: Frequency and percent distribution of employees' attitude towards InfoSec

Attitude	Frequency and percent
Positive	281 (95%)
Negative	15 (5%)
Total	***296 (100 %)***

Source: Questionnaire data, 2020

Table 9 above indicated that the majority 281 (95 %) of employees' have favorable attitude towards information security, while the remaining 15 (5 %) have a negative attitude towards information security. This implied that most employees of the agency believed that everyone in the agency has a role to play in protecting information against unauthorized threats, gave priority and great sort of attention to information conformation confidentiality, integrity, and availability to the right users.

4.1.4. The Level of Employees Perceived InfoSec Performance

Table 10. Employees Score on the Perceived InfoSec Performance Scale (N = 296)

Perceived InfoSec Performance	Frequency and percent
High	285 (96 %)
Medium	11 (4 %)
Total	***296 (100 %)***

Source: Questionnaire data, 2020

As indicated in Table 9 above, the majority of 285 (96 %) respondents have high perceived InfoSec performance, the remaining 11 (4 %) of participants have a medium performance. However, no participant has perceived his/her performance as low.

Most of the employees' perceived themselves as they have higher performance in using different information security measures such as strong passwords, shelf locks, etc. in their computers as well as document shelf. Regarding this, Pattinson and Anderson (2007) suggested

that the employees of the agency showed better practices in timely presenting the right files for the right users and places, keeping them integrated, and secreted to the right users.

Similarly, the INSA's Risk Assessment Team (2019) found that nearly 93 % of the agency's employees have strong InfoSec practices (used strong computer passwords, periodically changed it, and evaluate their practices towards information security performance indicators such as information confidentiality, integrity, and availability.

4.2. Differences in the Perceived InfoSec Performance as a function of Demographic Variables

4.2.1. Differences in Perceived InfoSec Performance by the Sex of Employees

Table 11: Independent t-test of perceived InfoSec performance as a function of employees' sex (N=296)

Dependent variable	Sex	*N*	*Mean*	*SD*	*t*	*P*
Perceived 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' perceived 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] *(See table 11 for mean, standard deviation, t-statistic, and p-value).* 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 males employees scored 2.21 standard deviation higher on the perceived InfoSec performance than females.

Besides, the Levene test result indicated that the assumption for equal variance was assumed [F (1, 294) = 27.5, p =.88] *(see Appendix 5A for Levene's test results of equality of variance)*, this means that the variances in male and female participants were not significantly different or variances in both sexes were approximately equal.

4. 2 .2. Differences in the Perceived InfoSec Performance by the Educational Level of Employees

Table 12: A one-way ANOVA analysis of perceived InfoSec performance as a function of employees' educational levels (N= 296)

Dependent variable	Educational Levels	*N*	*Mean*	*SD*	*Df*		*F*	*P*
					B/n groups	*W/in Groups*		
InfoSec Performance	Diploma	26	26.73	2.93	2	293	217.71	.000
	First degree	218	41.04	5.71				
	Second Degree	52	56.42	4.34				
	Total	***296***	***42.48***	***9.91***				

Source: Questionnaire data, 2020

To compare the perceived InfoSec performance as a function of employees' educational level, a one-way analysis of variance was performed. The comparison result revealed the existence of statistically significant InfoSec performance difference as a function of their educational levels [F (2, 293) = 217.71, $P < .05$, = .00, η^2= .60].

The Scheffe post hoc ANOVA result showed the existence of significant mean differences between diploma and first degree; diploma and second degree; and first degree and second degree *(See appendix 5B Scheffe post hoc ANOVA output).*

Generally, the result of comparison indicated that employees with higher educational levels can better protect the confidentiality, integrity, and availability of the agency's information than those of employees of lower educational levels (M= 56.42 for the second degree, M = 41.04 for the first degree, and M = 26.73 for diploma respectively) *(See table 12 above for means).* This means that employees with higher educational levels tend to periodically ensure the confidentiality of the information from unauthorized access, change, and deletion in the INSA context.

4.2.3. Differences in Perceived InfoSec Performance by the Job Position of Employees

Table 13: A one-way ANOVA analysis of perceived InfoSec performance as a function of employees' job position (N= 296)

Dependent variable	Job Position	*N*	*Mean*	*SD*	*Df*		*F*	*P*
					B/n groups	*W/in Groups*		
Perceived InfoSec Performance	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				
	Total	296	42.48	7.82				

Source: Questionnaire data, 2020

To test the employees' perceived InfoSec performance difference as a function job positions were tested using a one-way analysis of variance technique. The analysis result showed that employees' InfoSec performance was significantly differed by job positions they hold on [F (3, 292) = 46.59, P =.00, = .00, η^2= .324] *(See table 13 above for F statistics and P values).*

The Scheffe post hoc ANOVA result showed the existence of significant mean differences between the ordinary employee and supervisor position; ordinary expert and team leader; ordinary expert and director; supervisor and team leader; supervisor and director; team leader and director *(See appendix 5C Scheffe post hoc ANOVA output).*

Generally, the results of the mean comparison illustrated that employees with higher levels of job position tended to have higher scores of perceived InfoSec performance (M = 68 for the directors, M = 60.33 for the team leaders, M = 56 for supervisors, and M = 40.56 for an ordinary expert in descending order) *(See table 13 above for means).* This means that as the job position of employees changed from ordinary expert to supervisor, team leader, and director they used more information security tools such as encryption tools, software, passwords; periodically

check and evaluate the availability of files and documents in their computers and shelves; and can timely deliver them to the right users in electronic or printed form.

4.2.4. Differences in Perceived InfoSec Performance by the Length of InfoSec Training is taken by Employees

Table 14: A one-way ANOVA Analysis of perceived InfoSec performance as a function of the length of InfoSec training taken by the employees (N= 296)

Dependent variable	Length of InfoSec Training taken	*N*	*Mean*	*SD*	*Df*		*F*	*P*
					B/n groups	*W/in Groups*		
Perceived InfoSec Performance	3 days	93	30.34	3.78	2	293	846.19	.000
	1 week/5 days	116	44.07	2.19				
	6 months	87	53.34	5.22				
	Total	296	42.481	9.82				

Source: Questionnaire data, 2020

To examine the perceived InfoSec performance as a function of the length of InfoSec training taken by the employees, a one-way analysis of variance techniques was employed. The result showed that employees' InfoSec performance was significantly differed by the length of InfoSec training taken by the employees [F (2, 293) = 846.19, P =.00, = .00, η^2= .85].

The Scheffe post hoc mean comparison analysis result showed the existence of significant mean differences between employees who took 3 days of Infosec training and 1 week/5 day; 3 days, and 6 months; and 1 week/5days and 6 months of Infosec training *(See appendix 5E Scheffe post hoc outputs).*

In general, the mean comparison results implied that as the length of InfoSec training taken by the employees increased then their perceived InfoSec performance scores tend to increased (M = 53.34 for 6 months of InfoSec training, M = 44.07 for 5 days (1 week), and M =30.34 for 3 days in descending order) *(See table 14 above for means).* This means that employees who took the longest time of InfoSec training can better arrange files in their computer as well as

shelves and hide them from loss, unauthorized access, deletion, and changes, frequently monitor its availability, and contained appropriate backups.

4.3. The Relationship between the Predictor and Criterion Variables

Table 15: Summary of Pearson Correlations between the participants age, work experience, personality difference, attitude, and perceived InfoSec performance

N=296	Age	W.ex.	O	C	E	A	N	Att.	ISP
Age	1								
Work Expe.	.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		
Att.	.36**	.18**	.291**	.71**	.33**	.62**	-.37**	1	
ISP	.33**	.14**	-.099*	.61**	-.06	-.02**	-.54**	.59**	1

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

As shown in table 15 above, the perceived InfoSec performance scores of employees were positively related with age *(r (294) = .33, p < .01, r^2 = .11),* and work experience *(r (294) = .14, p < .01, r^2 = .019).* In addition, the perceived InfoSec performance scores of employees were positively related with conscientiousness (r (294) = .608, p < .01, r^2 = .37) and the attitude scores (r (294) = .593, p < .01, r^2 = .352). However, the perceived InfoSec performance scores of employees were negatively correlated with scores of openness (r (294) = -.099, p < .01, r^2 = .0098), extraversion (r (294) = -.055, p < .01, r^2 = .0030), agreeableness (r (294) = -.018, p < .01, r^2 = .000324), and neuroticism (r (294) = -.549, p < .01, r^2 = .30) *(See appendix 6 for effect size interpretations).*

Conscientiousness, attitude, openness, extraversion, agreeableness, and neuroticism effects explained 37 %, 35.2 %, .98 %, .3 %, .0324 %, 30 % of the total variance in the perceived InfoSec performance scores of employees, respectively. This means that conscientiousness,

attitude, and neuroticism have moderate effects on the perceived InfoSec performance scores of employees. Whereas, openness, extraversion, and agreeableness have small effects.

In other words, the magnitude of the correlation coefficients implied that conscientiousness (r = .608), neuroticism (r = -.549), and attitude (r = .593) were moderately correlated with the perceived InfoSec performance of employees in the INSA context. But, when conscientiousness and attitude positively related, while neuroticism was negatively related. Finally, the correlation coefficients (r = -.099 for openness, r = -.055 for extraversion, and r = -.018 for agreeableness) illustrated that being curious to know about many things, passionate and spirited with taking and discussing people, and trusting others have a small correlation with employees' perceived information confidentiality, integrity, and availability practices.

4.4. Predicting the Perceived InfoSec Performance of Employees' using the Predictor Variables

Table 16: Summary of the Hierarchical Multiple Regression results of personality difference and attitude in predicting the perceived InfoSec performance of employees of INSA (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
6	Attitude	.568	.012	3.26	2.89	.004	65.61	.004

Source: Questionnaire data, 2020

To predict the perceived InfoSec performance of employees using the predictor variables both separately and jointly, the hierarchical multiple regression analysis was employed. Independently, openness negatively predicted the perceived 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 the perceived InfoSec performance scores (β = .99, t (293) = 3.583, p < .01), as did attitude scores (β = 3.264, t (289) = 2.89, p < .01).

Generally, the standardized beta coefficients revealed that a change of one standard deviation in the openness, extraversion, agreeableness, neuroticism, conscientiousness, and attitude scores results in a change of -.38, -.113, -3.73, -3.7, .99, and 3.26 standard deviations in the employees perceived InfoSec performance scores respectively.

Jointly, the six predictor variables such as openness, conscientiousness, extraversion agreeableness, neuroticism, and attitude predicted the perceived InfoSec performance scores

of employees (R^2 = .568, F (6, 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 perceived InfoSec performances scores of employees both jointly and independently, conscientiousness improved prediction by (R^2 *change* = .417, F (1, 293) =19.13, p = .00, $\boldsymbol{f^2} = .81$), as did extraversion (R^2 *change* = .001, F (2, 293) = 72.796, p = .00, $\boldsymbol{f^2} = .001$), agreeableness scores (R^2 *change* = .024, F (4, 291) =59.865, p = .00, $\boldsymbol{f^2} = .025$), neuroticism scores improved (R^2 *change* = .113, F (5, 290) =75.147, p = .00, $\boldsymbol{f^2} = .13$), and attitude scores (R^2 *change* = .012, F (1, 289) = 65.611, p = .00, $\boldsymbol{f^2} = .012$). In terms of magnitude, conscientiousness was highly affected or improved prediction followed by neuroticism, agreeableness, attitude, and extraversion.

Generally, six independent variables jointly accounted for 56.8 % of the variance in the perceived InfoSec performance scores of employees in the INSA context. While 43.2 % of the variance in the perceived InfoSec performance of employees was explained by the unknown factors which were not included in the present study. Independently, openness, conscientiousness, extraversion, agreeableness, neuroticism, and attitude explained 1 %, 41.7 %, 0.1 %, 2.4 %, 11.3 %, and 1.2 % respectively.

Chapter Five

Discussion

In this chapter, the major findings of the present study were interpreted, discussed, and meanings were drawn in contrast to the existing body of literature. Therefore, the discussion was presented based on the sequence of the major research questions of the study.

5.1. The Level of Employees' Perceived InfoSec Performance

In this study, most employees of the agency have high perceived information security performance. This means that they used different information security measures such as strong passwords, shelf locks, etc. in their computers as well as document shelf to prevent their organization's information from unauthorized users, changes, and deletions. Regarding this, Pattinson and Anderson (2007) suggested that the employees of the agency showed better practices in timely presenting the right files for the right users and places, keeping them integrated, and secreted to the right users. Similarly, the INSA's Risk Assessment Team (2019) reported that nearly 93 % of the agency's employees have strong InfoSec practices (used strong computer passwords, periodically changed it, and evaluate their practices towards information confidentiality and availability).

Even though the data of this study was totally based on the perceived self-reports of the employees it contributed a clearer understanding of the level of employees' InfoSec performance in the Ethiopian, INSA context and builds existing evidence with empirical findings.

5.2. Differences in the Employees' Perceived InfoSec Performance as a function of their Demographic Variables

Concerning employees perceived InfoSec performance as a function of demographic factors such as sex, level of education, job position, and length of InfoSec training taken, the present study came up with statistically significant findings.

5.2.1. Perceived InfoSec Performance difference as a function of Sex of Employees

Regarding the perceived InfoSec performance difference by the sex of employees, a statistically significant finding was obtained. As the analysis of the independent sample t-test revealed that males and female employees were significantly varied in their perceived InfoSec performance scores. This means that males have relatively better InfoSec than female employees. In line with the present finding, Metalidoua et. al. (2014) and McCormac et. al. (2017) found that 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, these researchers were examined based on email phishing which totally depends on the electronic forms of InfoSec rather than being comprehensive. Meaning, information security performance trends in the physical or printed forms were not examined. Therefore, the present study was more comprehensive than the previous researchers by incorporating and examining the missed parts.

5.2.2. Perceived InfoSec Performance difference as a function of the Educational Level of Employees

The finding of the present study implied that the InfoSec performance of employees significantly differed by their level of educations. Regarding this, the one-way ANOVA computation revealed that as the employees' educational level increased, then their perceived InfoSec performance also increased. Also, the post hoc analysis shows that there was a statically significant mean score difference of InfoSec performance between the diploma and first degree; diploma and second degree; and first degree and second degree. This finding confirmed the research works of Tenney et. al., (2015) found employees with higher levels of education are less vulnerable to either electronic or printed form InfoSec problems. Because, as employees were educated more and more, they develop pragmatic skills, knowledge, awareness, and practices on how to keep the information secretly, in an organized and integrated manner, and use it with the right. Generally, this study provided a self-report and evidence-based understanding about the employees' perceived InfoSec performance difference as a function of their educational levels in the Ethiopian, INSA context.

5.2.3. Perceived InfoSec Performance difference as a function of Employees Job Position

Concerning the difference in the perceived InfoSec performance scores of employees by their job position, the present study found statistically significant results. That is directors, team leaders, supervisors, and ordinary employees perceived InfoSec performance significantly varied. Besides, statistically significant perceived InfoSec performance differences have been found between the ordinary employee and supervisor position; ordinary employee and team leader; ordinary employee and director; supervisor and team leader; supervisor and director; team leader and director in their perceived InfoSec performance measure.

The present study revealed that employees with a higher level of job positions tended to have higher perceived InfoSec performances than lower-level job positions. This finding was consistent with the existing body of research literature. For example, a study by Savola (2015) suggested that employees with higher positions (e.g. managers) are more conscious in making the information private, inaccessible to the authorized inside and outside users, used them properly when needed than the lower level position employees (e.g. juniors). Generally, this study contributed a self-report and evidence-based understanding about employees' perceived InfoSec performance difference as a function of their job position in the Ethiopian, INSA context.

5.2.4. Perceived InfoSec Performance as a function of Length of InfoSec Training taken by Employees

Looking at the employees' perceived InfoSec performance difference by the length of InfoSec training taken, the present study was found statistically significant results. As the analysis of one-way ANOVA showed that employees perceived InfoSec performance scores significantly differed by the length of InfoSec training, they took. This means that employees who took a longer InfoSec training tend to better secure the confidentiality, integrity, and availability of any information of the agency than those of participants who took a lower length of InfoSec training.

Moreover, a significant perceived InfoSec performance difference was obtained between employees who took 3 days of Infosec training and 5 days; who took 3 days and 6 months; and who took 5 days and 6 months of InfoSec training.

This finding confirmed various literature. For instance, Savola (2015) suggested that the length of the InfoSec training taken by the employees significantly relate to and predict their information confidentiality performance *(r = .58 and R^2 = .22).* Generally, this study provided a self-report and evidence-based understanding of the employees' perceived InfoSec performance difference as a function of InfoSec training taken in the Ethiopian, INSA context.

5.3. The Relationship between Predictor and Criterion Variables

To test the relationship between employees' age, work experience, personality difference, attitude, and perceived InfoSec performance, the Pearson correlation coefficient was performed. The result showed that employees perceived InfoSec performance positively related to age, work experience, conscientiousness, and attitude and negatively related to openness, extraversion, agreeableness and neuroticism.

To illustrate more, conscientiousness (being always prepared, organized, place computer and print files in a proper palace) and attitude (feeling responsible, and pay a great sort of attention to protect the agency's information from the illegitimate users) tend to maximize the confidentiality, integrity, and availability of information that they have in their own hands. 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 king for everyone) and neuroticism (lots of mood changes, easily disturbed, and emotionally unstable) tend to exposed the confidentiality, integrity, and availability of any files handled in their computer as well as file shelves.

This finding was consistent with the various research literature. For instance, Savola (2015) and Tenney et. al. (2015) found that employees with younger ages and lower years of work experience are more susceptible to InfoSec vulnerability problems than older ages and higher years of experience respectively.

McCormac et. al. (2017) found a positive association between conscientiousness and InfoSec performance in the confidentiality dimension (r = .37). In addition, Flowerday (2016), Iasi (2016), and McCormac et. al. (2017) found a positive association between the attitude and information confidentiality (r = .002, r = .71, and r = .23) respectively. Moreover, McCormac et. al. (2017) found openness (r = -.18), extraversion (r = -.12), and neuroticism (r = -.31) as negatively correlated with InfoSec performance in the information confidentiality. Also,

Parsons et. al. (2015) found a negative association between employees' InfoSec performance and their agreeableness personality type (being easily trusted and influenced by others) (r = -.01).

Also, in the present study, conscientiousness, neuroticism, and attitude moderately correlated with the perceived InfoSec performance of employees. In contrast, openness, extraversion, and agreeableness showed a small correlation with the scores of employees perceived InfoSec performance. Again, this finding was more or less consistent with the above-mentioned literature.

Even if the present study was consistent with previous findings, Flowerday's, Iasi's, and McCormac et. al.'s study were only based on a single dimension of information confidentiality. So, the present study was conducted by filling the gaps of those researchers, in that by including integrity and availability dimensions.

5.4. Predicting the Perceived InfoSec Performance of Employees' using the Predictor Variables

To predict employees of perceived InfoSec performance using the predictor variables both independently and jointly, a hierarchical multiple regression analysis was performed. Hence, the results of the present study revealed that the six predictor variables accounted for significant variance in the dependent variable both independently and jointly.

Openness, conscientiousness, extraversion, agreeableness, neuroticism, and attitude in combination explained significant variance in the employees' perceived InfoSec performance (R^2 = .568). Independently, openness, conscientiousness, extraversion, agreeableness, neuroticism, and attitude explained significant variations in the employees' perceived InfoSec performance, showed R^2 = .01, R^2 =.417, R^2 = .001, R^2 = .024, R^2 = .113, R^2 = .012 respectively. In other words, openness, conscientiousness, agreeableness, neuroticism, and attitude accounted 1 %, 41.7 %, 0.1 %, 2.4 %, 11.3 %, and 1.2 % of the variance in the employees perceived InfoSec performance respectively.

The finding confirmed the research works of Jain and Pal (2017) found that conscientiousness (employees' with more organized behavior) and attitude (favorable tendency and practice towards InfoSec) as the positive predictors of InfoSec performance in the information confidentiality dimension (showed 31 % and 29 %) respectively. However, as it is mentioned

in the above sections, Jain and Pal's study different from the present study in that it lacked comprehensiveness or lost information integrity and availability dimensions.

Chapter Six

Conclusion and Recommendation

6.1. Conclusion

Based on the findings and discussion of the study, the researcher draws the following conclusions with their corresponding implications:

Firstly, the results of the present study showed the majority of 285 (96 %) respondents have high perceived InfoSec performance, the remaining 11 (4 %) of participants have a medium performance. This implied that they used strong computer passwords and document shelf locks, they periodically changed it, timely present the right files for the right users and places, kept their files integrated, and periodically evaluate their practices towards information confidentiality, integrity, and availability.

Second, it was found out that employees perceived InfoSec performance significantly differed by their demographic factors such as sex, level of education, job position, and length of InfoSec training taken. This implied that as employees more educated, 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 usually used logging control for all folders and computer antiviruses; give number one priority for physical access control of any information in the agency; never share their passwords and file shelf keys even for co-workers etc.

Third, the results of the present study depicted that age, work experience, conscientiousness personality type፡ and attitude positively associated with the perceived information security performance of employees in the INSA context. This implied that employees with personality traits of being always prepared, preserved, planned, organized, scheduled, and have feel responsible and worry to protect the agency's information from illegitimate users tend to consciously check the subject and sender of the message in both electronic (e.g. email) and printed form (e.g. a letter), used multiple security control procedures (e.g., locking passwords, encryption, and other security settings), and periodically maintained the database and place of

documents in their computer or file shelves to keep the confidentiality, integrity, and availability of the information in electronic or printed forms.

In contrast, the result revealed that openness, agreeableness, extraversion, and neuroticism personality types were negatively associated with the perceived information security performance of employees in the INSA context. This implied that employees' with personality traits of being curious to know many things, trying to new things, focused on tackling new challenges; highly sociable, interactive; sympathize with others' feelings, trusting others, trying to make others happy, considerate and kind to almost everyone; and easily disturbed, experience worries, stress, and frequent mood shifts were unlikely to periodically check and evaluate their files at hand, use different security tools or settings such as computer passwords, folder locks, file shelf keys, and encryptions. On the other hand, even if they have some simple, weak or guessed passwords, they are more likely to share it with others around them and can randomly lose their file shelf keys. So that the files, manuals, or any workplace information in their responsibility may be exposed, lost, deleted, changed, modified, or unavailable to the right users and place.

Finally, the findings of this study revealed that the six predictor variables significantly predicted the criterion variable both independently and jointly. That is independently 1 %, 41.7 %, 0.1 %, 2.4 %, 11.3 %, and 1.2 % of the variance in the employees' perceived InfoSec performance was accounted for by a unit of change in the employees' openness, conscientiousness, agreeableness, neuroticism, and attitude scores respectively. Jointly, 56.8 % of the variance in the employees' perceived InfoSec performance was accounted for by a unit of change in the employees' openness, conscientiousness, agreeableness, neuroticism, and attitude scores together. However, 43.2 % of the variance was explained by the unknown factors which were not included in the present study.

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

6.2. Recommendation

Based on the conclusion of the present study findings, the researcher forwarded the following recommendations.

First, INSA's human resource recruiters and psychometrists should consider candidates with higher conscientiousness personality type and positive attitude when hiring for information security-related job positions.

Second, employers and organizations working with information security-related issues are advised to review the implications of relevant theories, models, and empirical evidence about personality difference, attitude, and information security performance, so that they can easily recruit, hire, and place the right personnel in the right position particularly in information security-related positions.

Third, even though the data of this study was perceived self-report based and has its own weakness and the recommendation raises ethical issues, the recruiters also need to consider the background characteristics such as sex, age, educational level, work experience, and length of InfoSec training taken by their candidates.

Fourth, psychologists or any other trainers working with the information security performance of employees need to consider the influence of personality difference and attitude on InfoSec performance and design and provide appropriate content and magnitude of training for employees with different personality types and attitudes.

Fifth, interventionists working with maximizing the InfoSec performance of employees need to pay adequate attention to employees with openness, extraversion, agreeableness, and neuroticism personality types and work hard to limit the negative impacts of these specific traits on InfoSec performances.

6.3.1. Recommendations for Future Research

This study has also important implications for future research. For instance, it should be conducted by expanding its scope or incorporating more demographic variables such as type of discipline that participants studied, colleges/facilities, religion, and other psychological variables such as motivation, belief, etc.

In addition to the self-report, future research must be conducted with triangulated data such as observation, interview, and focus group discussion (FGD) data.

Ended, since this study was conducted based on the perceptions or views of the employees, future research must be tested with the actual information security performance measures (e.g. employees information security performance records, performance evaluations, and other documented sources) than the perceived self-report measurements.

References

Ada, S., Sharman, R., & Gupta M. (2009). *Theories Used in Information Security Research*: Social organizational liabilities in information security. State University: NY.

Aellik, W. (2016). Personality Dimensions Across Cultures. *Journal of personality psychology, 24 (3),* 321–329. DOI: 18.418/9738-1-606566-132-2

Ahlan, A. R., Lubis M., & Lubis, A. R. (2015). Information security awareness and attitude at the knowledge-based institution: Its antecedents and measures. *Journal of Computer Science, 72,* 361 – 373

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

Ajzen, I. (1991). Theory of planned behaviour perspective. *Journal of Organisational Behavior, 50 (2),* 179–211.

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

Allport, W. (1937). What is a trait of personality? *Journal of Abnormal and Social Psychology, vol. 25,* 388–399.

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:* First order vs. second-order: Proceedings of the 32nd International Conference on Information Systems, Shanghai

Barrick, M. R. Mount, M. K., and Judge, T. A., (2001). Personality and performance at the beginning of the new millennium: What do we know and where do we go next? *International Journal of Selection & Assessment, 14 (9),* 36 - 48

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.* DOI:10.1371

Carlos, F. J. (2002). *An Introduction to information security performance measurement using balanced scorecards:* Global Information Assurance Certification Paper. SANS Institute

Computer Security Institute (CSI), (2012*). Computer security and crime survey.* Greenwich

Computer Security Team (CST), (2019). *Annual computer security internal report*. Addis Ababa, INSA

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

Eber, B., & Ttsuoka, M. (2016). *The personality factor questionnaire*. Champaign, IL.

Endirias, G., (2019). Facebook Usage and Psychosocial Well-Being among Private Preparatory School Adolescents in Addis Ababa. Master's thesis: Addis Ababa University

Flowerday, S. V. (2016). Ignorance to awareness: Towards an information security awareness process. *Journal of South African Institute of Electrical Engineers, 104 (2)*

Grazziano, A. (2015). Conscientiousness and driving accident involvement. *Journal of Personality Psychology, (94),* 648–659

Gundu, T. (2015). *Individuals' beliefs on information security threat controllability. School* of Informatics School, Malaysia

Hadlington, L. (2017). *Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours, 23 (4),* 236-248. DOI: 10.1016/j.heliyon.2017.00346

Harrison, A. A., Newman, D. A., & Roth, L. (2011). *The implication of attitudinal factors on Information Security.* NY

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

Herath, T., & Rao, H. (2009). Encouraging information security behaviours in the organization: the role of penalties. *Journal of Decision Support System, 5 (14), 154–165.*

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

Iasi, A. C. (2016). *Scales for measuring perceived information security risk in e-commerce:* Testing influences on reliability. University of Patricia, Elena

Information Security Forum (ISF), (2003). The standard of good practice for information security: *Information Security Forum-Standard Practices.* Florida, Orlando

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.

Joseph, P. S. (2016). *An empirical analysis of socio-cognitive factors affecting security behaviours and practices of smartphone users.* Doctoral dissertation. South Eastern University, Nova

Karwowski, W., & Glaspie, H. (2018). *Human factors in information security culture:* A literature review. DOI: 10.1007/978-3-319-60585-225

Kaur, J., & Mustafa, N. (2013). *Examining the effects of knowledge, attitude and behaviour on information security awareness: The 3rd International Conference on Research and Innovation in Information Systems (ICRIIS'13)*

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

Kruger, A. (2011). *Assessing information security Practices. Computers & Security, 25 (4),* 289-296.

Kruger, H., & Kearney, W. (2015). Information security issues. *Journal of Computers Security, 5 (78), 289-296.*

Kuusisto, T., & Ilvonen, I. (2010). Information security culture in small and medium-sized enterprises. Journal of Frontiers of e-business, *67 (23),* 431-439

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.

Li Meng, G., & Mincong, M. (2013). Information security engineering: A framework for research and practices. *International Journal of Computer Communication, 8 (4),* 578-587

Logistics and Supply Management Team (LMT) (2019). Annual logistics and supply management internal report. Addis Ababa, INSA

Maçada, A. (2015). Attitude and its implications in information security issues. *Journal of Social Psychology, 98 (1),* 214–228

Magana, W., and Lios, F. (2015). *Understanding attitudes and predicting behaviour.* Prentice-Hall, Englewood Cliffs, NJ.

Marczy, G., DeMatteo, D., & Festinger, D. (2005). *Essentials of research design and methodology*. New York

McCormac, A., Cali, D., Butavicius, M., Parsons, K., & Pattinso, M., (2017). Information security awareness and bias. *Journal of Information Systems, 36 (21),* 156-167

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M., (2017). Individual differences and information security awareness. *Journal of Computers in Human Behavior.* DOI: 10.1016/j.chb.2016.11.065.

McCrae, A., (2017). Patterns of personality traits in issues of information confidentiality. *Journal Applied Psychology, 3 (49),* 98–109.

Mekovec, R., & Hutinski, Z. (2015). *The role of perceived privacy, personality, and perceived security in the online market.* University of Zagreb: Organization and Informatics Faculty

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 attitude, behaviour and susceptibility to information security: *Journal of applied psychology, 114 (12),* 455–463

Mohannak, L. & Alfawaz, K. (2014). Information security with human factors. *Journal of Indian computer society, 39 (67),* 47–55.

Muellerleile, L., & Albarracin, B. (2016). A Meta-analysis on theories of reasoned action and planned behaviour Models. *Journal of the psychological bulletin, 127,* 142–161.

Munyoka, W. & Maharaj, M. S. (2019). Privacy, security, trust, risk, personality, and optimism bias in government organization information use. *South African Journal of Information Management, 21(1),* 967- 983

Nelson, C. & Yorke, L. (2015). The five-factor model: Investigating personality and 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. Kathryn Control, Communications, and Intelligence Division Defence Science and Technology Organisation: Australia

Pattinson M., Butavicius M., Parsons K., & Jerram C., (2015). Examining attitudes toward information security behaviour using mixed methods. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance* (*HAISA),* 57 (45), 138 - 149

Pattinson M., Parsons K., McCormac A., & Cate Jerram C., (2015). Determining employee awareness using the human aspects of information security questionnaire. *Journal of computers & security*, 101 (78), 267 - 278

Pervin, L. A., & John, O. P. (2016). *Handbook of personality*: Theory and research. New York: Guilford Press.

Posthumus, S., & Solms, R. (2012). A framework for the governance of information security. *Journal of Computers & Security, 79 (67),* 638-646.

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

Risk Assessment Committee Report (RACR) (2016). *An assessment of information security risks in the Ethiopian Management Institute (EMI).* Addis Ababa, Ethiopia

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)*

Siponen, M. T. (2000). *A conceptual foundation for organizational information security awareness. Journal of Information Management & Computer Security, 5 (3), 31-41.*

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

Tawileh, A., Hilton, J., & McIntosh, S. (2011). *Managing information security in small and medium-sized enterprises:* A Holistic Approach. *Europe Information Security Solutions Conference, 5 (45),* 331-339.

Teijlingen R. and Hundley V., (2014). Why a pilot study? *Journal of Applied Psychology*. DOI: 10.1823/206198.

Teru1, S. P., Hla, D., Idoko, I., & Tafida, A. (2016). The efficiency of accounting information systems and information security investment impact on a firm's performance. *European Journal of Business and Management, 8 (29),* 55-68

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

Warrington, C. (2017). *Personality trait and employee's information security behaviour*. Ph.D. dissertation: University of Capella

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

Witt, A., Barick, M., & Lointi, L. (2016). Information security practice, behaviour, and personality difference. *Journal of Applied Psychology, 23 (19),* 217- 228

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

Appendixes

Appendix 1: Questionnaire (English version)

Addis Ababa University

College of Education and Behavioral Studies

School of Psychology

Questionnaire to be filled by the Employees of INSA

Dear respondents, I am a postgraduate Social Psychology student at Addis Ababa University. Currently, I am doing a master thesis entitled *'personality difference and attitude associated with the perceived information security performance of employees in INSA''.*

The purpose of the study is for the fulfillment of the Master of Arts Degree in Social Psychology at Addis Ababa University.

To complete the questionnaire approximately 30 minutes will be taken. Since participation is voluntary, you are free to leave items blank that you do not want to answer. Also, you are free to withdraw from completing the questionnaire at any time with no penalty.

All information obtained from this study will be kept strictly confidential.

Finally, I (researcher) kindly requested you to give your genuine responses to each item in the questionnaire, because your genuine responses significantly matter the success of this research.

Thank you in advance for your cooperation and genuine response!

PART 1: Background Information

DIRECTION: The following items require you to provide information about you. Please read each and fill it properly.

1. Sex_____
2. Age_____
3. Level of education:

    Certificate ☐

    Diploma ☐

    First degree ☐

    Master's degree ☐

    PhD ☐

    other_____

4. Work experience in INSA (in years) _____
5. Job position:

    Ordinary expert/employee ☐

    Supervisor ☐

    Team leader ☐

    Director ☐

    other____

6. Length of information security training taken (in hours, days, months, or years) _____

PART 2: Big Five-Factor Inventory

DIRECTION: The following section contains items that can help to measure your personality. After reading each statement carefully, indicate your level of agreement by circling in one of the boxes under the alternatives given.

1 = Strongly Disagree ***2 = Disagree*** ***3 = Agree*** ***4 = Strongly Agree***

No	**Items**	**Level of agreement**			
Openness					
1	I am curious to know about many things	1	2	3	4
2	I am quick to understand things	1	2	3	4
3	I prefer work that is routine (R)	1	2	3	4
4	I have a vivid imagination	1	2	3	4
5	I am full of ideas	1	2	3	4
Conscientiousness					
6	I am always prepared	1	2	3	4
7	I persevere until the task is finished	1	2	3	4
8	I often forget to put things back in their proper place (R)	1	2	3	4
9	I make plans and follow through them	1	2	3	4
10	I make a mess of things (R)	1	2	3	4
11	I do things effectively and thoroughly	1	2	3	4
Extraversion					
12	Usually, I start conversations first	1	2	3	4
13	I am quiet around strangers (R)	1	2	3	4
14	I feel comfortable around people	1	2	3	4
15	I am passionate and spirited with people	1	2	3	4

16	I see myself as someone who is reserved (R)	1	2	3	4
Agreeableness					
17	I sympathize with others' feelings	1	2	3	4
18	I am not interested in other people's problems (R)	1	2	3	4
19	I am generally trusting others	1	2	3	4
20	I am considerate and kind to almost everyone	1	2	3	4
21	I am sometimes rude to others (R)	1	2	3	4
22	I like to cooperate with others	1	2	3	4
Neuroticism					
23	I am relaxed and can handle stress well (R)	1	2	3	4
24	My mood changes a lot	1	2	3	4
25	I often feel blue	1	2	3	4
26	I am easily disturbed	1	2	3	4
27	I am emotionally stable and not get stressed out easily (R)	1	2	3	4

PART 3: Attitude towards InfoSec (HAIS) measure

DIRECTION: The following 15 items are used to measure your attitude towards information security in the workplace. Please genuinely indicate your level of agreement by circling in the alternatives given below.

1 = Strongly Disagree ***2 = Disagree*** ***3 = Agree*** ***4 = Strongly Agree***

No	**Items**	**Level of agreement**
1	I believe that I have the responsibility to protect the agency's information from illegitimate users	1 2 3 4
2	I believe that everyone in the agency has a role to play in protecting against threats from information theft criminals	1 2 3 4
3	Information security issues should not be a priority within the agency (R)	1 2 3 4
4	I don't pay attention to the information security threats in the agency (R)	1 2 3 4
5	It's a bad idea to share my work passwords and file shelf keys, even if a colleague asks for it	1 2 3 4
6	I think it is necessary to use strong passwords or locks for my files at work	1 2 3 4
7	It is unlikely that my confidential information will not be stolen by illegitimate users at the workplace (R)	1 2 3 4
8	I believe that making the information confidential, integrated, and timely available when needed is important	1 2 3 4
9	I feel that my practice in handling sensitive information is appropriate and effective	1 2 3 4
10	In my view, using a password-protected computer and the locked shelf is a wise idea	1 2 3 4
11	Information security should be part of key performance evaluations for the employees of the agency	1 2 3 4
12	I worry about the information being exposed	1 2 3 4

13	I consider the privacy practices of the agency when sending, receiving, and storing any information	1 2 3 4
14	I feel safe with secured information on my computer or shelf	1 2 3 4
15	It’s nothing if the information that I manage is seen by others (R)	1 2 3 4

PART 4: Perceived Information Security Performance Scale (ISPS)

DIRECTION: The items below are used to measure your perceived InfoSec performance in the agency. Please, read carefully and honestly indicate your level of agreement in each item by circling one of the choices under the alternatives given.

1 = Strongly Disagree ***2 = Disagree*** ***3 = Agree*** ***4 = Strongly Agree***

No	**Items**	**Level of agreement**
1	I use computer antiviruses, file shelf locks to prevent important information from disclosure	1 2 3 4
2	On my computer, unauthorized employees can not access the agency's information resources	1 2 3 4
3	Logging all access attempts of confidential files and folders is mandatory	1 2 3 4
4	Physical access control is my number one priority	1 2 3 4
5	I do not share my passwords or key with colleagues so that I can protect the privacy of the information from unauthorized use	1 2 3 4
6	Usually, co-workers obtain my work-related information without authorization (R)	1 2 3 4
7	To increase the accuracy and reliability of the information, I periodically maintained the database and place of documents on my computer or file shelves	1 2 3 4
8	I used multiple security control procedures (e.g., locking passwords) to prevent unauthorized information change, add, and deletion	1 2 3 4
9	I always maintained the integrity of the information in electronic or printed forms	1 2 3 4
10	I use information security tools such as encryption and other security settings	1 2 3 4
11	I did not check and evaluate the integrity of information in my computer (R)	1 2 3 4
12	Sometimes, I lost the information that has been asked by the right users for a certain purpose (R)	1 2 3 4

13	The legitimate users can continuously access the information available in my hand	1	2	3	4
14	The probability of information system breakdown and information service disruption in my computer is low.	1	2	3	4
15	I always check the presence of the information in my hand	1	2	3	4
16	When acquiring important information from any sources or coworkers, I stored it in the agency's information database or secured shelf for later use	1	2	3	4
17	I frequently took a backup or copy of the information	1	2	3	4

Again, thank you for your cooperation!

አባሪ 2: መጠይቅ (አማርኛ ትርጉም)

አዲስ ኣባባ ዩንቨርስቲ

የትምህርትና ስነ-ባህሪይ ጥናቶች ኮሌጅ

የሳይኮሎጂ ትምህርት ቤት

በ INSA ሠራተኞች የሚሞላ መጠይቅ

የተከበራችሁ የዚህ መጠይቅ ተሳታፊዎች፥ እኔ በአዲስ አበባ ዩኒቨርሲቲ የማህበረሰብ ስነ-ልቦና የድህረ ምረቃ ተማሪ ነኝ ። በአሁኑ ጊዜ *"የሠራተኞች የስብዕና ልዩነቶች እና አመለካከት ከመረጃ ደህንነት አፈፃፀማቸው ጋር ያለው ዝምድና በኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ (ኢመድኤ)"* በሚል ርዕስ የሁለተኛ ዲግሪ መመረቂያ ፅሁፌን እየሰራሁ ነው።

የጥናቱ ዓላማም በአዲስ አበባ ዩኒቨርሲቲ በማህበረሰብ ስነ-ልቦና ሁለተኛ ዲግር ማሟያ ነው።

መጠይቁን ለማጠናቀቅ በግምት 30 ደቂቃዎችን ይወሰዳል። ተሳትፎው በፈቃደኝነት ስለሆነ እርስዎ መመለስ የማይፈልጓቸውን ጥያቄዎች ባዶ መተው ይችላሉ ። እንዲሁም ያለምንም ቅጣት መጠይቁን ከመሙላት በማንኛውም ጊዜ ለማቋረጥ ነፃ ነዎት።

ለዚህ ጥናት የተገኙት ሁሉም መረጃዎች በጥብቅ ሚስጢር ይያዛሉ ።

በመጨረሻም እኔ (ተመራማሪ) ለእያንዳንዱ ጥያቄ እውነተኛ ምላሽዎን እንዲሰጡ በአክብሮት እጠይቃለሁ። ምክንያቱም ለዚህ ምርምር ስኬት የእርስዎ እውነተኛ ምላሾች ትልቅ ዋጋ አላቸው።

ለትብብርዎ እና ለትክክለኛ ምላሽዎ እናመሰግናለን!

ክፍል 1. አጠቃላይ መረጃ

መመሪያ: የሚከተሉት ጥያቄዎች ስለእርስዎ አጠቃላይ መረጃ ይጠይቃሉ። እባክዎን እያንዳንዳቸውን ያንብቡ እና በትክክል ይሙሉ ።

1. ፆታ_____

2. ዕድሜ_____

3. የትምህርት ደረጃ:

   የምስክር ወረቀት ☐

   ዲፕሎማ ☐

   የመጀመሪያ ዲግሪ ☐

   ሁለተኛ (ማስተርስ) ዲግሪ ☐

   ሶስተኛ (ዶክትሬት) ዲግሪ ☐

   ሌላ_____

4. የስራ ልምድ (በዓመት)_____

5. የስራ መደብ:

   ባለሙያ ☐

   አስተባባሪ ☐

   ቡድን መሪ ☐

   ዳይሬክተር ☐

   ሌላ___

6. የወሰዱት የመረጃ ደህንነት ስልጠና እርዝመት (በቀን፥ ሰዓት፥ በወር፥ ወይም በአመት) _____

ክፍል 2: የስብዕና መለኪያ መሳሪያ

መመሪያ: የሚቀጥለው ክፍል የእርስዎን ስብዕና ለመለካት የሚረዱ ጥያቄዎችን ይዟል። እያንዳንዱን ዓረፍተ-ነገር በጥንቃቄ ካነበቡ በኋላ በተቀመጡት አማራጭ ሳጥኖች ውስጥ አንዱን በማክበብ የስምምነትዎን መጠን ያመልክቱ።

1 = በጣም አልስማማም 2 = አልስማማም 3 = እስማማለሁ 4 = በጣም እስማማለሁ

ተ.ቁ	ጥያቄዎች	የስምምነት መጠን			
ክፍትነት					
1	ብዙ ነገሮችን ለማወቅ እጓጓለሁ	1	2	3	4
2	ነገሮችን በፍጥነት መረዳት እችላለሁ	1	2	3	4
3	መደበኛ/የተለመደ ሥራን እመርጣለሁ	1	2	3	4
4	ግልፅ የሆነ የመገመት ችሎታ አለኝ	1	2	3	4
5	በሀሳቦች የተሞላሁ ነኝ	1	2	3	4
ጠንቃቃነት					
6	ሁል ጊዜ ዝግጁ ነኝ	1	2	3	4
7	ሥራ እስኪጠናቀቅ ድረስ በፅናት እሰራለሁ/ፅኑ ነኝ	1	2	3	4
8	ብዙውን ጊዜ ነገሮችን በተገቢው ቦታ ማስቀመጥ ረሳለሁ	1	2	3	4
9	እቅዶችን አወጣለሁ እነሱንም እከተላለሁ	1	2	3	4
10	ነገሮችን አዘበራርቃለሁ/አበላሻለሁ	1	2	3	4
11	ነገሮችን ውጤታማ በሆነ መንገድና በደንብ አደርጋለሁ	1	2	3	4
ውጫዊነት					
12	አብዛኛውን ጊዜ መጀመሪያ ውይይቶችን እጀምራለሁ	1	2	3	4
13	በእንግዳ ሰዎች አካባቢ ስሆን ዝም እላለሁ	1	2	3	4
14	በሰዎች ዙሪያ ስሆን ምቾት ይሰማኛል	1	2	3	4
15	አፍቃሪና አነቃቂ ነኝ	1	2	3	4
16	ራሴን እንደ ቁጥብ ሰው አድርጌ አየዋለሁ	1	2	3	4
ተስማሚ/ስምምነት					
17	ለሎች ስሜት ሩህሩህ ነኝ	1	2	3	4
18	የሌሎች ሰዎች ችግር ላይ ፍላጎት የለኝም	1	2	3	4

19	በአጠቃላይ ሌሎችን አምናለሁ	1	2	3	4
20	ለሁሉም ሰው በሚባል ደረጃ አሳቢ እና ደግ ነኝ	1	2	3	4
21	አልፎ አልፎ በሌሎች ላይ እበሳጫለሁ	1	2	3	4
22	ከሌሎች ጋር መተባበር እወዳለሁ	1	2	3	4
የስሜት አለመረጋጋት					
23	ዘና ያልሁና ውጥረትን በተገቢው ሁኔታ መቋቋም እችላለሁ	1	2	3	4
24	ስሜቴ በጣም ይቀያየራል	1	2	3	4
25	ብዙ ጊዜ የደበዘዘ ስሜት ይሰማኛል	1	2	3	4
26	በቀላሉ እረበሻለሁ	1	2	3	4
27	በስሜት የተረጋጋሁና በቀላሉ ውጥረት ውስጥ አልገባም	1	2	3	4

ክፍል 3: የአመለካከት መለኪያ

መመሪያ: የሚከተሉት 15 ጥያቄዎች በስራ ቦታ ላይ እስስዎ ለመረጃ ደህንነት ያልዎትን አመለካከት ለመለካት ያገለግላሉ። እባክዎትን ከዚህ በታች በተሰጡት አማራጮች መሰረት አንዱን በማክበብ የስምምነትዎን መጠን በትክክል ያመልክቱ።

1 = በጣም አልስማማም 2 = አልስማማም 3 = እስማማለሁ 4 = በጣም እስማማለሁ

ተ.ቁ	ጥያቄዎች	የስምምነት መጠን			
1	የኤጀንሲው መረጃ ከህገ-ወጥ ተጠቃሚዎች የመጠበቅ ሃላፊነት እንዳለብኝ አምናለሁ	1	2	3	4
2	በኤጀንሲው ውስጥ እያንዳንዱ ሰው የመረጃ ስርቆት ወንጀለኞችን ከመረጃ ስርቆት አደጋዎች ለመከላከል የሚጫወተው ሚና እንዳለው አምናለሁ	1	2	3	4
3	በኤጀንሲው ውስጥ የመረጃ ደህንነት ጉዳዮች ቅድሚያ ሊሰጣጨው አይገባም	1	2	3	4
4	በኤጀንሲው ውስጥ ለመረጃ ደህንነት ስጋቶች ትኩረት አልሰጥም	1	2	3	4
5	ታላላቅ ኩባንያዎችና ከፍተኛ የአስተዳደር ሰራተኞች ብቻ የመረጃ ስርቆት ወንጀለኞች ኢላማ እንደሆኑ አምናለሁ	1	2	3	4
6	በስራ ላይ ላሉኝ ፋይሎች ጠንካራ የይለፍ ቃሎችን ወይም መቆለፊያዎችን መጠቀም አስፈላጊ እንደሆነ አስባለሁ	1	2	3	4
7	በስራ ቦታ ምስጢራዊ መረጃየ ህጋዊ ባልሆኑ ተጠቃሚዎች ላይሰረቅ ይችላል	1	2	3	4
8	መረጃን ሚስጥራዊ፣ የተደራጀና ባስፈለገ ጊዜ ወቅታዊ በሆነ መልኩ ማዘጋዘትና ማቅረብ ጠቃሚ ነው ብየ አምናለሁ	1	2	3	4
9	እኔ እንደሚሰማኝ ወሳኝ መረጃዎችን በመያዝ ረገድ የእኔ ልምምድ ተገቢ እና ውጤታማ ነው	1	2	3	4
10	በእኔ እይታ በይለፍ ቃል የተጠበቀ ኮምፒተርንና የተቆለፈ መሳቢያን መጠቀም ብልህነት ነው	1	2	3	4
11	የመረጃ ደህንነት ጥበቃ ለኤጀንሲው ሠራተኞች ቁልፍ የሥራ አፈፃፀም ብቃት መገምገሚያ አካል መሆን አለበት	1	2	3	4
12	ደህንነቱ ስለተጋለጠ መረጃ እጨነቃለሁ	1	2	3	4
13	ማንኛውንም መረጃ በምልክበት፣ በመቀበልበትና በማከማችበት የኤጀንሲው የግል ሚስጥራዊ አሰራሮችን ከግምት ውስጥ አስገባለሁ	1	2	3	4
14	በኮምፒዩተሬ ወይም በሳቢያየ ውስጥ ደህንነቱ የተጠበቀ መረጃ ላይ ደህንነት ይሰማኛል	1	2	3	4
15	እኔ የማስተዳድረው መረጃ በሌሎች ቢታይ ምንም አይደለም	1	2	3	4

ክፍል 4: የመረጃ ደህንነት አፈፃፀም መለኪያ

መመሪያ: ከዚህ በታች ያሉት ጥያቄዎች እርስዎ በኤጀንሲው ውስጥ የእርስዎን የመረጃ ደህንነት አፈፃፀም ለመለካት ያገለግላሉ። እባክዎን በጥንቃቄ ያንብቡና የመረጃ ደህንነት አፈፃፀምዎን በሐቀኝነት ከታች ከተሰጡት አማራጮች መካከል አንዱን በማክበብ የስምምነትዎን መጠን ያመልክቱ ።

1 = በጣም አልስማማም 2 = አልስማማም 3 = እስማማለሁ 4 = በጣም እስማማለሁ

ተ.ቁ	ጥያቄዎች	የስምምነት መጠን			
1	ጠቃሚ መረጃዎችን እንዳይጋለቱ ለመከላከል የኮምፒተር ፀረ-ቫይረሶችን ፣ የፋይል መደርደሪያ ቁልፎችን እጠቀማለሁ	1	2	3	4
2	በኔ ኮምፒውተር ያልተፈቀደላቸው ሰራተኞች የኤጀንሲውን የመረጃ ሀብቶች ማግኘት አይችሉም	1	2	3	4
3	ሁሉንም የሚስጥር ፋይሎችን እና አቃፊዎችን ለማግኘት በመዳረሻ ሙከራዎች መግባት ግዴታ ነው	1	2	3	4
4	የአካል ተደራሽነት ቁጥጥር ቁጥር አንድ ቅድሚያ የምሰጠው ጉዳይ ነው	1	2	3	4
5	የመረጃውን ግላዊነት ካልተፈቀደ አጠቃቀም ለመጠበቅ የይለፍ ቃሎቼን ወይም ቁልፍን ለባልደረቦቼ አላጋራም	1	2	3	4
6	ብዙ ጊዜ የሥራ ባልደረቦች ከሥራ ጋር የተያያዙ መረጃዎችን ያለፍቃድ ያገኙብኛል	1	2	3	4
7	የመረጃውን ትክክለኝነትና አስተማማኝነት ለማሳደግ በየጊዜው በኮምፒተርሬ ወይም በፋይሌ መደርደሪያዎቼ ውስጥ የመረጃ ቋቴንና የሰነዶችን ቦታ እፈትሻለሁ	1	2	3	4
8	ያልተፈቀደ መረጃን መለወጥን ፣ መጨመርንና መሰረዝን ለመከላከል ብዙ የደህንነት ቁጥጥር አሰራሮችን (ለምሳሌ ፣ የይለፍ ቃላትን) እጠቀማለሁ	1	2	3	4
9	በኤሌክትሮኒክ ሆነ በታተመ ይዘት ሁልጊዜ የመረጃውን ታማኝነት አረጋግጣለሁ	1	2	3	4
10	ምስጠራና ሌሎች የመረጃ ደህንነት ቅንብር መሣሪያዎችን እጠቀማለሁ	1	2	3	4
11	በኮምፒውተሬ ውስጥ ያለውን የመረጃ ትክክለኛነት አልፈትሽም አልገመግምም	1	2	3	4
12	አንዳንድ ጊዜ ለተወሰነ ዓላማ በትክክለኛ ተጠቃሚዎች የተጠየቁትን መረጃ አጣዋለሁ	1	2	3	4
13	ህጋዊ ተጠቃሚዎች በእጄ ውስጥ ያለውን መረጃ በተከታታይ ማግኘት ይችላሉ	1	2	3	4
14	በኮምፒውተሬ ውስጥ የመረጃ ስርዓት ብልሽትና የመረጃ አገልግሎት መቋረጥ እድሉ ዝቅተኛ ነው	1	2	3	4
15	መረጃው ሁልጊዜ በእጄ ውስጥ መኖሩን አረጋግጣለሁ	1	2	3	4

16	ከማንኛውም ምንጮች ወይም ባልደረቦቼ ጠቃሚ መረጃዎችን በማገኝበት ጊዜ በኤጀንሲው የመረጃ ቋት ውስጥ ወይም ደህንነቱ በተጠበቀ መደርደሪያ ውስጥ በኋላ ላይ ለመጠቀም በሚያስችል መልኩ አስቀምጣለሁ	1	2	3	4
17	በተደጋጋሚ የመረጃውን የመጠባበቂያ ቅጂ ወይም ግልበጫ እይዛለሁ	1	2	3	4

ስለ ትብብርዎ በድጋሚ አመሰግናለሁ!

Appendix 3: Oral Consent Message (read for the participants)

Dear respondents, I am a postgraduate Social Psychology student at Addis Ababa University. Currently, I am doing a master thesis on the Five-factor personality and attitude associated with the information security performance of employees in INSA.

Purpose: One is for the fulfillment of the Master of Arts Degree in Social Psychology at Addis Ababa University, second is to assess the relationship and prediction between five-factor personality difference, attitude, information security performance of employees in INSA

The completion of the questionnaire will take approximately 30 to 45 minutes. Since participation is completely voluntary, you are free to leave items blank that you do not want to answer. Also, you are free to withdraw from completing the questionnaire at any time with no penalty.

Risks and benefits: There are no known risks associated with this study. The finding of this study may provide evidence-based information about the personality, attitude, and information security performance of employees of INSA for the internal and external scientific communities.

Confidentiality: All information obtained from this study will be kept strictly confidential, except as may be required by you and national law. Any information that could be used to identify you will be kept under lock, key, or secret. Data files will not contain potentially identifying information.

Consent: I have listened and understood the above information and I willingly consent to participate in this study. I understand that if I should have any questions about my rights as a research participant, I can contact the student researcher's advisor Dr. Dame Abera *at email: dame288@gmail.com*. I can also contact the principal researcher Mr. Anemut Mehari by *email: meharipsyc@gmail.com* or by phone at *(+251) 920246085.*

Appendix 4: SPSS outputs of Pilot study

Annex 4.1: Cronbach's Alpha and item-total statistics for Big-5 Factor scale & sub-scales

Scales		***No of Items***	***Cronbach's Alpha***
BFFI		28	.81
	Openness sub-scale	5	.90
	Conscientiousness sub-scale	6	.87
	Extraversion sub-scale	5	.91
	Agreeableness sub-scale	6	.75
	Neuroticism sub-scale	6	.81

Item-Total Statistics

	Items	***Scale Mean if Item Deleted***	***Scale Variance if Item Deleted***	***Corrected Item Total Correlation***	***Cronbach's Alpha if Item Deleted***
Openness	Item 1	10.3041	4.795	.637	.891
	Item 2	10.4088	4.527	.617	.892
	Item 3	11.1723	4.516	.676	.888
	Item 4	10.5304	5.077	.600	.893
	Item 5	10.6520	4.960	.668	.889
Conscientiousness	Item 6	12.1858	8.620	.706	.886
	Item 7	12.2905	8.248	.662	.889
	Item 8	13.0541	8.119	.542	.899
	Item 9	12.4122	8.948	.712	.886
	Item 10	12.5338	8.697	.709	.886
	Item 11	13.2669	7.356	.722	.821
Extraversion	Item 12	9.5709	5.886	.613	.863
	Item 13	9.6757	5.616	.612	.968
	Item 14	10.4392	5.474	.774	.847
	Item 15	9.7973	6.271	.793	.856
	Item 16	10.6520	4.960	.612	.954
Agreeableness	Item 17	12.1858	8.620	.781	.854
	Item 18	12.2905	8.248	.719	.786
	Item 19	13.0541	8.119	.641	.722
	Item 20	12.4122	8.948	.789	.751
	Item 21	12.5338	8.697	.601	.767
	Item 22	13.2669	7.356	.847	.714
Neuroticism	Item 23	9.3277	5.631	.687	.856
	Item 24	9.1959	5.155	.628	.786
	Item 25	9.5541	5.868	.727	.867
	Item 26	9.6757	5.616	.789	.851
	Item 27	9.4088	4.527	.707	.867

Annex 4.2: Cronbach's Alpha and item-total statistics for Attitude scale

Cronbach's Alpha	*No of Items*
.83	15

Item-Total Statistics

Items	*Scale Mean if Item Deleted*	*Scale Variance if Item Deleted*	*Corrected Item Total Correlation*	*Cronbach's Alpha if Item Deleted*
Item 1	34.7939	66.707	.863	.823
Item 2	34.8986	65.732	.813	.865
Item 3	35.6622	65.289	.789	.857
Item 4	35.0203	67.661	.713	.815
Item 5	35.1419	66.780	.763	.863
Item 6	35.8750	62.923	.914	.865
Item 7	34.7939	66.707	.783	.805
Item 8	34.8986	65.732	.883	.856
Item 9	35.6622	65.289	.649	.714
Item 10	35.0203	67.661	.883	.856
Item 11	35.1419	66.780	.629	.786
Item 12	35.8750	62.923	.746	.867
Item 13	35.1419	66.780	.847	.851
Item 14	35.8750	62.923	.608	.867
Item 15	34.7939	66.707	.747	.862

Annex 4.3: Cronbach's Alpha & item-total statistics for Perceived InfoSec Performance scale

Cronbach's Alpha	*No of Items*
.89	18

Item-Total Statistics

Items	*Scale Mean if Item Deleted*	*Scale Variance if Item Deleted*	*Corrected Item Total Correlation*	*Cronbach's Alpha if Item Deleted*
Item 1	39.6250	85.415	.910	.958
Item 2	40.3885	84.957	.727	.959
Item 3	39.7466	87.559	.607	.957
Item 4	39.8682	86.691	.744	.957
Item 5	40.6014	82.302	.641	.956
Item 6	39.5203	86.684	.924	.957
Item 7	39.6250	85.415	.741	.959
Item 8	40.3885	84.957	.674	.957
Item 9	39.7466	87.559	.841	.956
Item 10	39.8682	86.691	.924	.957
Item 11	40.6014	82.302	.910	.956
Item 12	39.5203	86.684	.627	.955
Item 13	39.6250	85.415	.707	.957
Item 14	40.3885	84.957	.844	.956
Item 15	39.7466	87.559	.841	.957
Item 16	39.8682	86.691	.824	.959
Item 17	40.6014	82.302	.741	.957

Appendix 5: Test of Equality of Variance Statistics

5A

Group Statistics					
	Sex	N	Mean	Std. Deviation	Std. Error Mean
InfoSec	Male	195	37.4514	7.47449	.53526
	Female	101	52.1781	5.64041	.56124

Levene's Test of Homogeneity of Variance					
		F	df1	df2	Sig.
InfoSec performance	Based on Mean	27.494	1	294	.8812

5B

ANOVA					
InfoSec					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	17012.401	2	8506.201	217.717	.000
Within Groups	11447.514	293	39.070		
Total	28459.916	295			

Post hoc Tests

Multiple Comparisons							
Dependent Variable: InfoSec							
	(I) Level of education	(J) Level of education	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower	Upper
Schef fe	Diploma	BA	-14.30593*	1.29689	.000	-17.4967	-11.1152
		MA	-29.69231*	1.50135	.000	-33.3861	-25.9985
	BA	Diploma	14.30593*	1.29689	.000	11.1152	17.4967
		MA	-15.38638*	.96466	.000	-17.7597	-13.0130
	MA	Diploma	29.69231*	1.50135	.000	25.9985	33.3861
		BA	15.38638*	.96466	.000	13.0130	17.7597

*. The mean difference is significant at the 0.05 level.

Test of Homogeneity of Variances					
		Levene Statistic	df1	df2	Sig.
InfoSec	Based on Mean	38.949	2	293	.000

5C

ANOVA

Infosec

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	9213.410	3	3071.137	46.594	.000
Within Groups	19246.506	292	65.913		
Total	28459.916	295			

Post hoc Tests

Multiple Comparisons

Dependent Variable: infosec

	(I) Job position:	(J) Job position:	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Scheffe	Ordinary employee	Supervisor	-15.38113*	1.92816	.000	-20.8029	-9.9594
		Team leader	-19.71447*	2.75179	.000	-27.4521	-11.9768
		Director	-27.38113*	4.71377	.000	-40.6356	-14.1267
	Supervisor	Ordinary expert	15.38113*	1.92816	.000	9.9594	20.8029
		Team leader	-4.33333	3.28523	.629	-13.5709	4.9043
		Director	-12.00000	5.04381	.132	-26.1825	2.1825
	Team leader	Ordinary expert	19.71447*	2.75179	.000	11.9768	27.4521
		Supervisor	4.33333	3.28523	.629	-4.9043	13.5709
		Director	-7.66667	5.41244	.572	-22.8857	7.5524
	Director	Ordinary expert	27.38113*	4.71377	.000	14.1267	40.6356
		Supervisor	12.00000	5.04381	.132	-2.1825	26.1825
		Team leader	7.66667	5.41244	.572	-7.5524	22.8857

*. The mean difference is significant at the 0.05 level.

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
InfoSec	Based on Mean	28.622	3	292	.000

5D

ANOVA

Infosec

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	24259.823	2	12129.911	846.187	.000
Within Groups	4200.093	293	14.335		
Total	28459.916	295			

Post hoc Tests

Multiple Comparisons

Dependent Variable: infosec

	(I) Length of InfoSec training taken	(J) Length of InfoSec training taken	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower	Upper
Scheffe	3 day	5 days	-13.7248*	.52699	.000	-15.0214	-12.4283
		6 months	-23.0074*	.56472	.000	-24.3901	-21.6114
	5 days	3 days	13.72488*	.52699	.000	12.4283	15.0214
		6 months	-9.27586*	.5398	.000	-10.5970	-7.9547
	6 months	3 days	23.00074*	.5472	.000	21.6114	24.3901
		5 days	9.27586*	.53698	.000	7.9547	10.5970

*. The mean difference is significant at the 0.05 level.

Test of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
InfoSec	Based on Mean	34.774	2	293	.000

Appendix 6: Effect Size Sample Formulas

Sample formulas for calculating effect size values

1. The effect size for significant t-test computed by Cohen's d:

$$\boldsymbol{Cohen's\ d = \frac{t\sqrt{n1 + n2}}{\sqrt{n1n2}}}$$

2. The effect size for significant ANOVA F computed by partial eta-squared:

$$\boldsymbol{Cohen's\ \eta p^2 = \frac{ssbg}{ssbg + sswg}}$$

3. The effect size for significant Pearson correlation coefficient of determination:

$$\boldsymbol{Cohen's\ r^2}$$

4. The effect size for significant R^2/regression coefficient of determination/ by:

$$\boldsymbol{Cohen's\ f^2 = \frac{R^2}{1 - R^2}}$$

Effect size specifications

	Symbol	***Small***	***Medium***	***Large***
t-test on means	*d*	.20	.50	.80
F-test ANOVA	ηp^2	.10	.30	≥ .50
Coefficient of determination in correlation	r^2	.10	.30	≥ .50
Coefficient of determination in multiple regression	f^2	.02	.15	.35

Source: Cohen (1988)

Magnitude of Correlation values: .30 small, .50 moderate, and .70 strong correlation coefficients

Address: Anemut Mehari <meharipsyc@gmail.com>