An-Najah National University

Faculty of Graduate Studies

Factors Influencing Employees on Compliance with Information Security Policies in Palestine

By

Bara Mohammad Abu Jafar

Supervisor

Dr. Mohammad Othman

Co-Supervisor

Dr. Abdel Fattah Hasan

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Engineering Management, Faculty of Graduate Studies, An-Najah National University, Nablus - Palestine.

2019

Factors Influencing Employees on Compliance with Information Security Policies in Palestine

By

Bara Mohammad Abu Jafar

This Thesis was Defended Successfully on 29/4/2019 and approved by:

Defense Committee Members	Signature
1. Dr. Mohmmad Othman / Supervisor	.....
2. Dr. Abdel Fattah Hasan / Co–Supervisor	.....
3. Dr. Fadi Shrouf / External Examiner	.....
4. Dr. Fadi Draidi / Internal Examiner	.....

Dedication

I would like sincerely to thank all my beloved family members especially to:

- My dear parents, who have given me the drive and discipline to tackle any task with enthusiasm and determination.
- Dear wife for her understanding, patience and continuous support.
- My Kid "’Mohammad" which his presence in my life motivate me always to strive for the best.
- Treasured Brothers and Sisters "Bilal, Abelrhaman, Obada, Osama, Wala" for their encouragement.

Acknowledgement

My deep gratitude to my family for their patience, encourage and support.

My sincere appreciation to my supervisors Dr. Mohammad Othman and Dr. Abdel Fattah Hasan for their efforts and guidance.

Many thanks to all of the referees who dedicated time for reading and commenting on the research questionnaire including

Dr. Yahya Saleh, Dr. Ahmad Awad, Dr. Suhel Salhaa, and Dr. Ayob Abed Alkareem.

الإقرار

انا الموقع أدناه مقدم الرسالة تحت عنوان:

Factors Influencing Employees on Compliance with Information Security Policies in Palestine

أقر بأن ما اشتملت عليه هذه الرسالة هو نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وأن هذه الرسالة لم تقدم من قبل لنيل أي درجة علمية، أو أي بحث علمي أو بحثي لأي مؤسسة تعليمية أو بحثية أخرى.

Declaration

The work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted elsewhere for any other degree of qualification.

Student's Name: اسم الطالب: براء محمد سلامة ابو صعر

Signature: التوقيع:

Date: التاريخ: 2019/4/29

Table of Content

List of Tables

List of Figures

List of Appendices

Abbreviations

Abbreviation	Construct/Variable
IF	Individual Factors
OF	Organizational Factors
ES	Employees Satisfaction
TWE	Technological Work Environment
IS	Information Security
ISCP	Information Security Compliance Policies
ISO	International Organization for Standardization
ISP	Information Security Policies
OPEN	Openness
CONS	Conscientiousness
EXTRA	Extraversion
AGRE	Agreeableness
NEUR	Neuroticism
MOR	Moral
SUPP	Support
CULT	Culture
TRAIN	Training

Factors Influencing Employees on Compliance with Information Security Policies in Palestine

By

Bara Mohammad Abu Jafar

Supervisor

Dr. Mohammad Othman

Co-Supervisor

Dr. Abdel Fattah Hasan

Abstract

Information security is very important and critical for organizations. Human error is the biggest threat to information security so organizations have to develop and improve employees' performance to comply with information security policies. The aim of this thesis is to study the potential factors affecting employees' compliance on information security policy. Therefore, this study is an explanatory research in nature. The target population for the study was Palestinian employees in Palestine who work with computers. Therefore, 500 questionnaires were distributed, but only 372 questionnaires were valid for analysis, with response rate 74.4%. A sample of 372 questionnaires has been distributed to several service organizations including universities, telecommunications and internet service providers companies, insurance companies and banks. Using Structural Equation Modeling-Partial Least Squares Method, the results indicated that individuals' factors of employees, organizational factors, and technological work and environmental factors have influence positively on information security compliance policies. Also, the results show that the older employees tend to comply with information security policies than younger employees throughout an organization. Moreover, gender factor

has no significant effect on Information security compliance policies. These findings are useful for organizations policy makers who plan to improve employees' compliance with information security polices, and researchers interested in information security polices compliance as well. Some recommendations were suggested to the organizations managers: increasing of organizational support for employees, conducting periodic training in information security, spreading the creativity and excellence amongst the employees, and providing a suitable and good environment for employees.

Chapter One
Introduction

1.1 Background

Securing certain kinds of information is necessary for corporates, agencies, and institutions. Leaking of confidential information may lead to several damages, mainly to reputation, credibility, and accreditation. Information Security (IS) intends to keep all electronic data under full and direct control, so that nobody other than the authorized can access or make changes to the secured data/information without formally obtaining prior permission. Human factors that influence (human) behavior have huge impact over computer security. They can be personality traits, cognitive abilities, individual differences and the unique level of risk perception of every associated individual. All the above-mentioned factors are in addition, influenced by the culture, technologies and security environments of an organization in which the breaches take place. When these factors collaboratively interact with each other, they induce adverse human behavior capable of destructing information security. The world has witnessed tremendous advancements in information sciences. However, they fail to ensure a 100% secured environment since the issues aren't solely technical and predominantly due to human factors. Computers' being exclusively operated by human beings is the most obvious reason. Human factors intrude with the way individuals' interact/communicate with IS technologies. It is apparent that technical solutions alone cannot entirely prevent information breaches. Hence organizations ought to

introduce a culture that values positive information security behaviors, amongst its workforce. Challenges that employees' encounter in using IS frameworks and technologies have to be identified and resolved. This implies that it is substantial for security functions to be more visible, meaningful, easy and convenient to locate and use. Providing intense behavioral training and educating employees on the significance of IS awareness, are the often-recommended actions against security breaches. The way in which, every individual interacts with computers, and makes decisions relating to information security has always been complex and dynamic. Hence the IS systems need to acknowledge, consider and scrutinize the human factors that influence. Also, there are heuristics and biases (favoritism or partiality) that affect the extent of risk an individual would be willing to take in certain situations; and examining via such a dimension could explain what made an individual take certain decisions while also observing specific behaviors. Individual differences and risk perception are both, also influenced by the operating environments of individuals. Climate and culture certainly has major impact on their behaviors, attitudes and values. This is exactly why it is essential to understand an organization's security and culture. They provide deeper insights into the foundation of certain behaviors. Today, the most serious concerns pertaining to Information Security are the threats imposed by 'Social Engineering' (SE) attacks. These attacks are executed to retrieve sensitive and confidential information and maliciously used against organizations and individuals. It is vital for individuals to be educated regarding such potential attacks and the use of appropriate tools that curtail

their probability of being affected. On the contrary, it is often the insiders who pose serious security risks, owing to their possession of legitimate/authorized access to information and facilities, location of assets and related organizational knowledge. They are capable of committing highly deteriorating security breaches while leaving very little evidence. Organizations however do not seem to employ adequate risk management systems that can withstand such situations (Colwill, 2009). Companies have largely been neglecting to realize the severity of human imposed challenges in effectively managing information security. In order to address these issues, the management needs to identify the skills essential for altering the organizational culture, enhance communication amongst senior managers, IS managers and end users, and allocate resources to jobs based on their individual identity (core values, beliefs, attitudes, personal and social elements) (Ashenden, 2008).The complexity and obscure nature of information security issues caused by human factors further emphasize the need for promoting positive IS behaviors besides improving the physical and technical aspects of computer security (Parsons et al., 2010).

Information security support and culture include the organizational and managerial characteristics that drive employee compliance with a security policy. A series of characteristics are examined in the literature that are shown to have a positive relationship with security policy compliance, including organizational factors (Chan et al., 2005; Goo et al., 2014; Hu et al., 2012), and security training (Bulgurcu et al., 2010; Lowry et al., 2015; Puhakainen & Siponen, 2010; Siponen et al., 2010). Security policy can

generate positive emotional and social outcomes, such as happiness (Siponen & Iivari, 2006), and job satisfaction (D'Arcy and Greene, 2014), these factors impact the degree that employees will comply with the guidelines. In contrast, security policies that contribute to stress (D'Arcy et al., 2014) and role conflict (Teh et al., 2015) are found to lead to non-compliance. A lot of factors examined in the security policy research include aspects of an individual's ethical standards, such as personal norms (Ifinedo, 2014), and morality (Hu et al., 2011; Myyry et al., 2009; Vance & Siponen, 2012).

The focal objective of this research is to select employees from service companies in diverse sectors and segregate them into Generation X, referring to those born within the years 1960-1979 and Generation Y, commonly referred to as the Millennial generation born within 1980-2000 (Reisenwitz et al., 2009); and determine their varied personality traits that are highly influential over their information security practices within their organizations. This will essentially include an acute investigation of human factors that are capable of affecting employee commitment and compliance within the sphere of their information security systems.

1.2 Research Problem

The whole world is evolving and progressing towards technology in a much faster fashion, and so should the organizations, in order to sustain the fierce competition today. This in turn mandates a constant upgrade in the performance of one of their high-priority functions, i.e. 'Information

Security', alongside finding a comprehensive and integrated system for protecting organizational data and information.

In around 80-90% of security related organizational accidents, the human factors are most certainly implicated (Gonzalez, & Sawicka, 2002). They can largely influence the levels of information security awareness amongst the employees of an organization (McCormac et al., 2017). The big five personality dimensions (Neuroticism, Extraversion, Openness, Agreeableness, Conscientiousness) also have considerable impact on employees' performance constructs relating to Information Security. Goo et al. (2014) and Hu et al. (2012) showed that the organizational factors and security training have a positive relationship with security policy compliance, while Chan et al. (2005) and Herath and Rao (2009b) and Hu et al., (2012) found the organizational support to be positively associated with compliance, but D'Arcy and Greene (2014) and Ng et al (2009) found that organizational support had either a negative or insignificant relationship to security behaviors. Some research findings link individual's factors to policy compliance are inconclusive (Goo et al., 2014), or show that it has an indirect influence on policy compliance (Posey et al., 2015), factors such as low self-control(Conscientiousness) is found to link negatively to policy compliance (Guo & Yuan, 2012; Hu et al., 2011, 2015; Ifinedo, 2014). To complicate further, the workforce of any organization consists of people from different generations with varying traits and personalities that should be considered within the subject of Information Security. Organizations that have engaged an ageing workforce might

experience a contrast pattern of security compliance issues, in comparison to those that have employed young employees. The older generation prefers to retain some information in order to distinguish it among the rest of the employees and this creates a knowledge gap between the older and younger generations. Some of the traits that employees from different generations may not have in common include openness, friendliness, co-operation, conscientiousness to voluntarily abide to security policies, etc. These varying traits have a negative impact over employees' compliance with the information security policies (Cram et al., 2017). Thus, understanding the relationships among human, organizational, technological and environmental factors and their influences on information security compliance policies is considered as a research opportunity.

1.3 Research Questions

1. What Factors of different generations' employees significantly influence their compliance with Information Security policies?

1.1. What Individual Factors of different generations' employees significantly influence their compliance with Information Security policies?

1.2. What Organizational Factors of different generations' employees significantly influence their compliance with Information Security policies?

1.3. What Technological Work Environment of different generations' employees significantly influences their compliance with Information Security policies?

1.4. What Employees Satisfaction of different generations' employees significantly influences their compliance with Information Security policies?

2. How do these identified Factors of different generations' employees interact with security compliance' constructs and influence them?

2.1 How do these identified Individual Factors of different generations' employees interact with security compliance' constructs and influence them?

2.2 How do these identified Organizational Factors of different generations' employees interact with security compliance' constructs and influence them?

2.3 How do these identified Technological Work Environment of different generations' employees interact with security compliance' constructs and influence them?

2.4 How do these identified Employees Satisfaction of different generations' employees interact with security compliance' constructs and influence them?

1.4 Research Objective

The objectives of this research project are:

1- Identifying the major Individual Factors, Organizational Factors, Technological Work Environment and Employees Satisfaction that influence different generations' employees towards complying with the organization’s information security policies.

2- Developing an empirical model that describes Individual Factors, Organizational Factors, Technological Work Environment and Employees Satisfaction that majorly influence security compliance of employees and exhibit their impact over various securities constructs of the organization.

1.5 Thesis structure

This study consists of five chapters. The first chapter is the introduction where the background, problem statement, research questions, research objectives and the scope of the study are introduced. Chapter two defines the concept of Individual and organizational factors and their different types, as well as introducing the literature review and summarizing the previous studies about Compliance with Information Security Policies.

The third chapter presents the research methodology and identify the research population, survey sample, data collection tool as well as the data analysis software packages used in analyzing the gathered data. Chapter four presents data analysis and discussion. Finally, chapter five is the conclusions and recommendations of this research.

Chapter Two
Literature Review

In this chapter, the theoretical background of the research is to be discussed in addition to literature review of the previous studies. Furthermore, Conceptual Framework and Hypothesis are presented.

2.1 Overview

Over the years, several researchers, computer engineers and scientists, and cryptologists have performed numerous empirical studies in specific sectors such as banks, telecommunication, and education sectors, etc..., to understand the difficulties of effectively managing the information security infrastructures of organizations. Their findings illustrate the need for robust IS systems with high-level standards that provides systematic approaches to adopt best breach control policies, practices, guidelines and procedures (Alshekh, 2015; Beautement & Sasse, 2009; Dey, 2007; Dynes et al., 2005; Siponen and Oinas-Kukkonen, 2007; Siponen & Willison, 2009).

2.2 Information Security

Every business immensely relies on ‘information’ of any related kind, which has today become its most valuable, vital and intellectual asset. The Information Security (IS) concept is basically the framework or system devised by an organization to safeguard this asset and ensure its availability only to the authorized. It protects the interests and concerns of people who depend on communication and information technology systems that manage and secure their data, and prevent from failing in terms of integrity,

availability or confidentiality of data-resource applications, databases or organization' websites (Mohsen, 2014; Oguk et al., 2017). Unsecured and leaked information could both due to misuse, cause loss of reputation and business to the organization. Since it makes the continued existence or survival of an organization questionable, Information Security is clearly a business related issue and not just technical. Hence IS issues should ideally be addressed by top-level management and executed with the involvement and support of downstream executives for assessing threats and effectively responding to them (Abu-Musa, 2010; Dey, 2007; Siponen, 2001).

2.3 Information Security Management

Information Security Management (ISM) system needs to be all encompassing and cannot merely be confined to a pack of software and hardware. Successfully establishing and implementing such a complete system demands participation, focus, and commitment from employees at all organizational levels (Dey, 2007). ISM is made of diverse aspects such as Information Security Policies, Risk Management, Risk Analysis, Disaster Recovery, and Contingency Planning (Feng et al., 2014; Solms et al., 1993). Since the above are interrelated, they often overlap and cause certain uncertainties while making crucial decisions. In addition, managing and training the employees in this perspective for avoiding spectacular failures can also be a critical challenge for any organization. There are several IS certification standards like ISO27001 and ISO9001 that are adopted within business environments for establishing, actualizing, executing, monitoring, maintaining, improving and reviewing security

frameworks which in unison, enhances quality of IS management systems. Organizations seek such certifications for varied purposes, e.g., it may be customer demanded, or for gaining a competitive advantage. Gillies (2011) supported the very robust ISO27001 standard and discovered that there were several barriers preventing organizations from adopting it. Evidence suggested that the adoption of ISO27001 was slower in comparison with other existing standards since it was complex and expensive for smaller organizations, faced difficulties in gaining support from senior-level management, etc. It's certain that organizations will be open to adoption of such quality enhancing certifications only when they seem to be easy and inexpensive transformations (Gillies, 2011). Employees are characterized with cautious behavior and security awareness, which imparts them with a major role in IS performance. They are expected to prevent unwanted incidents and protect the organization's material/immaterial assets. They can contribute even while performing routine day-to-day activities by locking their computers when they aren't using them, frequently changing their login credentials, avoiding the usage of unlicensed software and immediately reporting security breaches, if any (Albrechtsen, 2007).

2.4 Corporate Governance

Corporate Governance creates of the combination of procedures and internal controls by which organizations, irrespective of type or size, are managed and guided (Von Solms & Von Solms, 2006).

Corporate executives face more pressure with the rising awareness on the urgent need for highly effective corporate governance of IS. This is mainly because of threats from terrorists, globalization, and newly imposed government regulations demanding organizations to safeguard their data and constant growth in the level of dependence on Internet. The staggering reputational and financial loss incurred in the case of large-scale information breaches have pushed these executives to consistently rank privacy and information security as one of the core organizational issues. Hence many firms continuously strive to elevate their security functions by expanding budgets, evaluating based on the return on security investments, or hiring security experts, etc. However, the ultimate question that remains unanswered is what kind of IS approach or strategy will be the most effective? Originally it was more technology oriented and abandoned the people who were really the ones interacting with all those high-end systems. Today, experts suggest strategic Information Security approaches that aren't restricted to IT products/solutions (technically competent security specialists and sophisticated technologies) alone but also involve social alignment and organizational integration mechanisms. When the human element is combined with technology, the IS framework can be more socio-technically oriented and provides wider opportunities to explore the threats to data security. Benefits of employing this approach include greater compliance, improved alignment of security policies and spending with business, and reduced security breaches (Kayworth and Whitten, 2010).

The goal of behavioral aspects of security governance is to guarantee that employees show stratification with the regulations and policies. Since employees rarely comply with information security policies.

Procedures, particularly that involving information security, are seen as mere guidelines or general directions to follow rather than "hard and fast regulations" that are specified as standards (Herath & Rao, 2009).

2.5 Information Security Compliance

There are numerous researches that discuss the factors affecting employees' compliance with IS (Cram et al., 2017). Kim and Kim (2017) distributed a structured survey questionnaire to all the employees of S-OIL, a leading Korean energy company. Their study involves empirical examination of the voluntary efforts made by employees, to maintain compliance levels in proportion with level of information technology utilization. For this purpose (encouraging employee compliance), they suggest the use of knowledge management systems/strategies that offered compliance self-assessment tools, support for compliance-related tasks, compliance trends monitoring, educational programs and information sharing for employees. By promoting an intention to comply with information security systems amongst employees, the growth of organizations can be made more sustainable. The aim of behavioral aspects of security governance is to ensure that employees show conformity with the rules and policies. Since employees rarely comply with information security procedures. Policies, especially those involving information

security, are viewed as mere guidelines or general directions to follow rather than “hard and fast rules” that are specified as standards (Herath & Rao, 2009). According to Ifinedo (2012) due to the relatively discretionary nature of adherence to policies, organizations find enforcement of security a critical challenge. Thus more recently, research in behavioral information security has started focusing attention to employee intentions to follow security policies. In organizational information security, responsibility of whether to adhere to organizational security policies or ignore them is delegated to employees. Employees may choose to break security policies for malicious purposes or choose to avoid security policies for mere convenience (Herath et al., 2010). In conclusion, when the intentions are strengthened by positively influencing employees’ attitudes, the actual level of compliance automatically escalates (Siponen et al., 2006).

2.6 Human Factors

Several studies suggest that human factors have predominantly been responsible for leaking of secured information. Ashenden (2008) deemed human factor to be the most serious challenge faced by any organization, and that the managing of relationships amongst them is even more difficult. Effective Communication can eliminate most of the issues around the role of human factors in Information Security was the author’s theory. The findings of Colwill (2009) affirm that insiders of an organization can often cause considerable harm. The fact that security experts/officers were more concerned over outsider threats in comparison with those within the organization was also exposed when investigations revealed that 82% of

employees in charge of making security decisions' were unaware of their organization's source of insider risk; and around 5830 spyware/malware attacks actually originated from within the company. Colwill (2009) pointed out that the denial of existence of threats from the insiders can only result in detrimental failures. McCormac et al. (2017) examined the link between employees' IS awareness and their distinct variables such as age, personality, risk-taking propensity and gender, for finding ways to facilitate tailored security training and imparting more awareness on the consequences of security breaching. In order to assess the employees' IS awareness, a 'KAB-Knowledge, Attitude and Behavior' model was used; and for measuring the same, a 'Human Aspect of Information Security' Questionnaire (HAIS-Q) based on KAB model was employed. Also, they used the 'Big Five Personality Model' for understanding and predicting the human factors that employees might encounter within complex and diverse environments. The 5-factor personality model is one of the prominent theoretical models focusing on understanding and measuring varied personalities. Its 5 factors include openness, conscientiousness, extraversion, neuroticism and agreeableness. The study revealed that emotional stability, risk-taking propensity, conscientiousness and agreeableness of individuals caused significant variance in there awareness levels; and recommended that adequate training may be provided to employees in a much tailored way, to identify and focus on each of their individual strengths and weaknesses. Behavioral outcomes of employees that have a major say in securing an organization's information resources, are a result of employee intentions and attitudes. However intentions

cannot be totally accepted as an ideal predictor of their actual behavior, because not always do employees act according to their intentions. This gap in between intentions and actual behavior is possibly due to certain variables; and personality constructs seem to majorly contribute. Hence Shropshire et al. (2015) devised a conceptual model to study the contribution of personality traits (agreeableness and conscientiousness) and attitudinal traits (perceived organizational support, ease-of-use & usefulness), in influencing the decision of individuals to act or not on their intention to engage themselves in protective/secure behaviors. For this purpose, 170 undergrad participants from a famous US University were provided with internet-based security software that can be used to evaluate the vulnerabilities of their own computers; following which, the conceptual model was employed to conduct an in-depth assessment of traits that caused them to adopt/neglect the software. Results revealed that greater conscientiousness-oriented traits in people made them more self-disciplined, cautious and use the security software voluntarily; and greater agreeableness-oriented traits in people made them more easily influenced by peer encouragement in adopting the security software. It also claimed that perceived ease-of-use and usefulness positively influenced behavioral intention, while organizational support failed to do so (Shropshire et al., 2015).

2.6.1 The Five- Factors Models of personality: definition and description

The Five Factors Model (the Big 5) is considered the most suitable and widespread modern psychology model due to its five factors which offer precise personality description. According to Digman (1990), these traits are the most practical among existing measures within personality psychology (Abadu, 2013). The Five Factor Model aims at piecing together the many traits under basic categories which stay fixed as main factors, whether we add to them or extract from them. These traits are indispensable in any description of the human personality. The Five Factor model is based on the idea that individual differences, which indicate daily interaction among people, will be a language registered people use to communicate.

Almawafi and Radi (2006) stated that psychology aims to establish a model suitable to describe the human personality, and use it in diagnosing and treating personality disorders. Digman (1990) noted that models which describe the human personality are limited, adding that the most widely acceptable one is the Big 5 model; a highly applicable and practical model in psychology (Almawafi & Radi, 2006).

The Big 5 is considered the most up to date modal in personality description. It is a comprehensive model concerned with describing and classifying personality trait terminology which differentiate people from one another (Saucier, 2002). Some of the most important models dealing

with the five factors of personality are documented in Digman (1990), Costa and McCrae (1995), and Coldberg (1992). The main factors underlying the hierarchical structure of the five traits include agreeableness, neuroticism, extraversion, openness on experience, and conscientiousness (Lindend et al., 2010).

The Big 5 Model is a hierarchical structure of human traits. The five factors represent the summit of the hierarchy, with personality as the highest level, each having bipolar dimension as extraversion-introversion. The bipolar lie beneath the five traits in the hierarchy, with more specific dimension for each factor (Gosling, et al., 2003). Following is a definition and description of these factors.

Factor one: Neuroticism

Neuroticism is a factor contrasting between compromise, maturity and emotional stability, with non-compromise. Neuroticism is not neurosis; it is the predisposition to develop the condition once pressure and neurotic situations are present (Abdelkhaliq, 1998).

Neuroticism, which is the opposite of emotional stability, reflects individual trends towards emotional instability, dissatisfaction, and difficulties in adjusting with others. Neuroticism is also associated with anxiety, shyness, guilt, pessimism, grief and self-disrespect (Da Raad, 2000; Zhang, 2009).

Neuroticism is negatively associated with life satisfaction and positively with expressing one's self on fatigue. Neurotic people have less ability to work under stress, and have less control over their impulses. Costa and McCrae (1995) described the neurotic person as one who has high levels of anger experiences, disgust, sorrow, confusion and negative reactions.

Factor two: Extraversion

This factor forms a bipolar with introvertedness. An extraverted person loves being around others, complies with external standards, directs interest towards others, likes working with others, and respects traditions and authority. At the level of thinking, this person relies on logic in explaining worldly events and lives within fixed practical, objective or ideological rules. An extravert is gentle, optimistic, cheerful, and enjoys life (Costa & McCrae, 1995). An introvert, on the other hand, directs interests and emotions inwards towards him/herself, and is sensitive despite hiding in feelings. At the level of thinking, an introvert explains special ideas based on his/her special rules, and has a strong need for secrecy "privacy" (Zhang, 2006: 1179; DeRaad, 2000: 89).

Factor three: Agreeableness

This factor is the most closely linked to personal relations. According to Hogan (1983), agreeableness makes an individual capable of facing life problems and pressures; it reflects individual differences in reaching social harmony. People having this trait are tolerant, trustworthy, good natured, cooperative, and accept and respect others (DeRaad, 2009; Zhang, 2006).

It seems that people with high levels of agreeableness have a tendency to overexert themselves to help and please others, such as co-workers, friends and family (Bruk & Allen, 2003). Agreeableness was divided to many levels. On one extreme is the meek and adapting personality which submits its own needs for the needs of others, and accepts the standards of the group instead of insisting on its own personal standards. At the highest level of this extreme is a subservient self-denying person. The meek personality is most suitable for social roles as teaching, social work and psychology. On the other extreme we find the challenging personality, which focuses on its own standards and needs. Such a personality can become narcissist, selfish and skeptical (AlSalem, 2006).

Goodness is associated with positive personality variables including achievement, persistence, responsibility, and organization. People with such traits always aim for achievement through social compatibility (Ewen, 1998).

Factor four: Openness to experience

Open people are mentally curious, have a taste for art, and a sense of aesthetic awareness. These people tend to be emotionally conscious compared to introverts; they tend to think and act via individual, non-identical modalities. However, people who are closed to experience tend to have narrow mutual interest. They prefer simplicity, directness and clearness to complexity, and vagueness. They look upon art and science skeptically, and view them as difficult or useless efforts. Closed people

prefer common to new and resist change. Conservative closed thinking is associated with the work of the police and sales (AlAnzi, 2007).

Howard & Howard (1995) added that openness to experience is characterized by having many interests, being liberal and capable of thinking and criticizing. It indicates principles along with the acceptance of new methods. In contrast, people closed to experience have limited interests, uphold traditions, and feel relaxed with the familiar, but not necessarily authoritarian. Such a person is suitable for roles of a financial manager, project manager, and scientists in the field of applicable sciences. Between these two characters, we find moderate personalities capable of detecting new and necessary interests, despite that excessive focus can exhaust them. They are able to focus on familiar things for a long time, but creativity and innovation will result eventually (Al-Saleem, 2006).

Openness to experience includes constant search, liking of new experiences, openness, creativity, belief in a just world, mental engagement, and the need for aesthetic sensitivity, non-dominating values, and openness to others' feelings and emotional experiences (Haredi & Shawqi, 2002).

Factor five: Conscientiousness

Dedication contributes to how we control and organize our incentives. Incentives are not inherently bad; sometimes time constraints require immediate decisions. Working on our first incentive is a form of effective response. Dedication includes a factor known as the need to achieve and

accomplish, leading to visible benefits. Dedicated people avoid problems, reach high levels of success through targeted planning and persistence, and people trust them and see them as intelligent persons. The negative shade of such personal trait is becoming a perfectionist, compulsive and work addict. People see such persons as deranged, boring, and in some cases untrustworthy and non-ambitious, (AlAanzi, 2007).

According to Howard & Howard (1995) high dedication "conscientiousness" indicates focus, while low dedication indicates a spontaneous, superior unfocused person with multi goals. This prevents such persons from relaxing from time to time and enjoying life (AlSalem, 2006).

2.6.2 Work Ethics

The basis of work ethics is based on mutual relations between colleagues and employees (Vance & Siponen, 2012). The most prominent factors examined in the security policy research include aspects of an individual's ethical standards, such as personal norms (Ifinedo, 2014), morality (Hu et al., 2011; Myyry et al., 2009; Vance & Siponen, 2012). Greenberg (2002) found that employees at the conventional level of moral reasoning were less likely to steal from their employers – especially when they worked in an office with an ethics program – than employees at the preconvention level.

According to the Myyry et al. (2009), there are some Value types:

1- Achievement: personal success and competence according to social norms (successful, capable, ambitious, Influential).

2- Benevolence: protecting the welfare of close others in everyday interactions (helpful, forgiving, honest, loyal, responsible).

3- Tradition: respect, commitment, and acceptance of the customs and ideas that one's culture or religion imposes on the individual (accepting one's share in life, devotion, respect of tradition, humility, moderation).

4- Conformity: restraint of actions, inclinations, and impulses likely to upset or harm others, or violate social expectations or norms (obedience, self-discipline, politeness, honoring parents and elders).

2.7 Organizational Factors

Information security culture, awareness, and support includes the organizational and managerial characteristics that drive employee compliance with a security policy. A series of characteristics are examined in the literature that are shown to have a positive relationship with security policy compliance, including organizational values, climate, and norms (Chan et al., 2005;Goo et al., 2014; Hu et al., 2012).

2.7.1 Training

The definition of training varies following the various viewpoints. It is defined as regulated procedures which enable an individual to gain skills or

new knowledge that helps him/her achieve goals, it is also known as "planned and organized efforts by the organization to equip workers with certain knowledge and enhance and develop their competences and abilities, and change their attitudes constructively" (Almosawi, 2004). Sekiou (1999) considered training to be "connected with human resource management, and it is a series of processes and methods which help develop workers' knowledge, behavior, viewpoints, and mental abilities necessary for achieving the goals of both the organization and the individual". Training is part of continuous learning which aims at enabling human resources to adapt with changing technology and changing work conditions. It is a means to promote methods of social advancement through reaching different levels of culture, thus contributing to cultural, economic, and social development (Peretti, 2005). Sekiou (1999) considered training a way to nurture the human resource's self-respect, thus trust in one's self is gained and positive attitudes are created. It also leads to having the right person for the right job, so the worker will carry out tasks assigned to him/her faster, avoiding work accidents (Sekiou, 2004). Cadin (2002) listed the following goals for training:

1- Enhance individual and group performance of human resources.

2- Develop production capacity.

3- Change human resources' organizational culture to confirm with the organization's goals.

4- Enhance and develop adaptation and resist non-adaptation (Cadin, 2002).

Thereby, the main aim of training is to ensure compatibility between human resources and organization needs. Experts in human resource management assure the necessity to enhance competences within the organization, and this can be achieved only through training.

The main principles of training can be summarized as follows:

1- Aim: this needs be precise and clear and follow personnel needs.

2- Continuity: this is achieved when training starts with the start of the work life, and continues step by step to develop personnel following the developmental needs.

3- Inclusiveness: training must include all job levels and all hierarchical levels in the organization.

4- Progressivity: training starts solving simple issues and then progresses towards more problematic issues.

5- Keeping pace with evolution: so that training is a source of new and up to date benefit for all workers.

6- Realism: training needs to fulfill actual trainee needs and suit their levels (Altaani, 2007).

2.7.2 Support

Eisenberger et al. (1990) defined individual awareness of organizational support as the level at which workers recognize that the organization cares for them, values their efforts and looks over them. George (1999) defined support as the degree to which the organization cares for its workers and their prosperity through treating them equally, helping them in facing problems and listening to their complaints. Support is perceived by Singh and Malhorta (2015) as workers' beliefs that the organization values their efforts to achieve its success. The philosophy of the idea of perceived organizational support is psychological; it can be perceived as loyalty of the organization for its workers. When workers are aware of their organization's support, they become loyal (Shore & Tetrick, 1991) However, individual awareness of organizational support varies from one worker to another, and this awareness is based on a number of factors including the organization's willingness to provide support or basic tools so workers can perform at the highest levels; its willingness to provide training opportunities, encourage workers continually, value their efforts, and give them the chance to be part of the decision making process (Eisenberger, 1997).

Types of perceived organizational support:

1- Supervisory support: This refers to exchange between the individual and the supervisor. It is based on the social exchange theory and the principle of reciprocity. It states that basic human exchange started through exchange

of resources. It suggests that the exchange between individuals and supervisors is based on weighing benefits and costs of the exchange from a personal perspective. If benefits outweigh risks and cost which the employee bears, he/she will proceed with this relationship. The principle of reciprocity indicates that employees feel committed to good treatment in line with the treatment they receive from their supervisors.

Tekleab and Chiaburu (2011) saw that supervisory support gives the employee a clear understanding of the organization's support. Studies indicate that supervisors are capable of achieving organization policy through cooperation with employees, and at the same time they submit periodic reports on goal achievements and the role of each employee in reaching goals creating strong relations between supervisors and employees.

2- Co-worker support: Employees view the organization as a human being, thus they perceive its actions as human actions. Likewise, organization agents' actions represent the organization. The term agent does not only refer to supervisors and presidents; it includes coworkers, thus agency relationships link the organization with the employees. From the employee's perspective, s/he has agency relationships with two parties: supervisors and coworkers. Consequently, any analysis of organizational support must not be limited to the organization alone; it needs to include all agents as supervisors and coworkers. Positive coworker relations lead to positive stances towards perceived organizational support. Moreover, dominating relations among workers perform a number of functions. The

most important function is psychological and social support coworkers for the employee. This is due to the fact that workers believe that their coworkers live under the same condition as theirs, making them more capable of understanding their feelings and concerns at work (Zumrah, 2014).

2.7.3 Organizational Culture

Hareem (2010) have defined organizational culture as "something similar to the culture of the society as it includes beliefs, assumptions, values, rules, standards and other shared man-made behavioural patterns. Organizational culture is the personality and the climate of an organization, and it determines its behavior, suitable connections and encourages individuals. Hareem and Alsaaed (2006) defines organizational culture as "the assumptions, beliefs, values, rules and standards which people of an organization share; it is the humanitarian environment within which the employee does his/ her job". Culture is intangible and invisible, yet it is present everywhere in the organization and affects it.

Alkhafaki (2009) considered culture as shred values encompassing the basic beliefs which help the organization in seeking excellence. Al-Qariuti (2000) summarizes the importance of organizational culture as follows:

1- It is a guide for both administration and employees as it shows must-follow behaviors and relations.

2- It is an intellectual framework which directs and organizes the members of the organization, their relations and their achievements.

3- Workers inside an organization do not perform their roles individually; they perform under a single regulatory body. Thus, culture and the values and behavioral rules it includes, indicate the expected organizational behavior, and the relationship patterns between workers, the organization agents and other bodies they deal with. This includes dress code, appearance and language.

4- A strong organization culture is an effective factor supporting and helping the management in achieving its goals and ambitions. It also makes easier the tasks of the management and team leaders as they will not need strict formal procedures to affirm the required behavior.

5- It offers a competitive advantage for the organization since it emphasizes creative behavior as dedication at work and in client service. However, it can become detrimental once emphasizing routine behavior as total obedience and strict commitment to formalities.

6- It is an essential factor in attracting suitable workers, as pioneer organizations attract ambitious workers, and organizations adopting values of innovation and excellence appeal to innovative workers. Additionally, hardworking and self-motivated employees are likely to join organizations which reward excellence and development.

7- Culture is considered as a vital element affecting the organization's acceptance of change and its ability to keep pace with developments. The more flexible the organization's values are and the more forward looking they are for the better, the more capable they are in achieving change and the more keen they are to benefit from that change. On the contrary, fixed, conservative and consistent values, result in an organization unready and less capable of development.

The culture of any organization, like any other aspect, requires efforts which maintain its stability and have a lasting impression on the lives of their employees, thus they follow instructions related to behavior and relations.

- Types of organizational culture:

Many researchers have tried to analyze organizational culture which differs among organization and sectors following the basics of division. The many types of organizational culture include the following (AlAhmed, 2008; Alsarayra, 2003; Daft, 2004).

1- The degree at which the dominating organizational culture can reflect its true needs (Handy's Model), and this includes:

- Power culture: this indicates centralization in decision-making, and limiting authorities to senior management, while other managements are executive powers only. This is usually the case of small sized

organizations, and problems emerge when the organization grows and the management finds itself unable to keep all authorities in its hands.

- Role culture: this culture focuses on career specialization. It adds focus to regulations and rules, dislikes risk, and assures job security, continuity and consistent performance. Role culture's primary problem is being suitable during times of stability, which are very rare.

- Task culture: this culture focuses on achievement and task accomplishment via optimal utilization of resources to achieve the best results with least expenses.

- Process culture: this is limited to the method through which tasks are achieved regardless of the results. The successful employee is the most accurate and organized in details of the daily occupation.

- Achievement culture: the organizational culture focuses on levels of success, growth and excellence of its employees. Organizations possess an achievement culture if they rely on the achievement consolidation via motivations, honoring ceremonies, certificates of appreciation…etc. which increase employee enthusiasm to achieve excellence.

2- Organizational culture following administrative leadership patterns (Walsh's Model):

- Bureaucratic culture: responsibility and authority are set out hierarchically and based on monitoring, control, power and obligation (work is organized and coordination is apparent).

- Innovative culture: this culture provides a work environment supporting innovation not only through focus on additional improvements which can be added to the organization, but also through focus on organizations from which employees can learn that failure is the key to success. These employees are risk takers in the decision making process and in facing challenges to create a new way of work which leads the organization to more growth and development.

- Supportive culture: also known as the culture of human compassion as it focuses on social relations and a work environment of intimacy and friendliness. An atmosphere of trust, equality, cooperation, justice, fairness and safety prevails the organization.

3- Organizational culture based on employees' attitudes within their organizations (John's Model):

- Capital culture: the focus of this culture is on employees' attitudes towards the work they do to avoid weakness. The organization needs to offer sufficient guarantee for employees to carry out the work with no tiredness nor fragility.

- Professional culture: This is characterized by skills and general specializations as it is based on reciprocal leadership instead of official authority, rules and procedures.

4- Organizational culture based on strength and weakness (Luthans' Model):

- Strong culture: it builds strong connections between members of an organization and indicates members' commitment to values and beliefs. It has been agreed on that individuals are defined by the common values of their organization, and that incentives and motivations are to be awarded to committed employees.

- Weak culture: employees walk an ambiguous path, with unclear features. They receive contradicting instructions, thus fail in taking the right decision.

5- Organizational culture is based on adaptation with the organization's environment (Daft's Model):

- Adaptability culture: this focuses on the external environment as the organization tries to adopt a method of flexibility and change in order to address customer needs via innovation and development.

- Mission culture: the focus is on the clarity of the mission with regard to the organization's goal, and goal fulfillment. The focus is on a particular sector of customers within the external factor with no need for rapid change as profitable sales growth or market share.

- Clan culture: the basic focus is on the engagement and participation of individuals within the organization, and speed in implementing expected change in the external environment.

- Bureaucratic culture: The main concern is internal environment integrity and stability, which leads to high levels of obedience and cooperation among individuals.

To summarize, organizational culture with its definition, importance, aspects, elements, durability and interaction with other organizational elements directly affects individual and group behavior within the same organization and with other organizations. Absurd and non-systematic methods and behaviors negatively affect the organizations productivity and efficiency. Moreover, negative individual behavior results in negative coworker behaviors. Organizations strive to allocate great importance to organizational culture so as to create individual and administrative innovations capable of keeping the organization standing on its feet in the face of ongoing change.

2.8 Work environment (presence of suitable conditions and tools):

Work environment is the environment related to the organization itself regarding administrative and substantive frameworks, formal and non-formal systems, organizational structures and implementation procedures, technologies used, mainstream communications… etc.

2.8.1 Technologies used within organizations:

This refers to cognitive and technical inputs applied to reach final or intermediate outputs. These can enrich the inputs of other organizations (Maher, 2010).

2.8.2 Regulations governing organization-employee relations

The application of regulations depends on administrative powers allocated to the manager or administrator. Application of regulations faces a number of constraints and obstacles which prevent the achievement of expected results or contribute to the emergence of issues and problems that strangle the organization's work and cause employee disengagement. One case of disengagement is negative rejection or resistance due to the nature of the regulations and the procedures adopted in their application. This results in tension and division among employees (Saeed, 1987).

2.8.3 Communication within the organization

Communication is defined as the transfer of information between two or more individuals to raise understanding, exchange viewpoints, or coordinate intellects and behavior. The organization conducts a wide range of communications through which it can give distinct features to its work procedures and its administration. The aim is to raise employee loyalty and belonging (Alkbesi & Amer, 1998).

2.8.4 Work nature

Work nature refers to methods and means adopted in the implementation of personnel policy within the administration. It also includes procedures and organizational measures which serve both organization and employee goals (Alamro, 1996).

The physical conditions of work and their effects:

Physical conditions are considered one of the most essential elements of a work environment. They refer to conditions that face an employee during the work execution process (Mashaali, 2011). These include the following:

1- Lighting: this is considered the production unit at a work place, as eyes send 85% of what senses perceive to the central nervous system. Vision enables shape, color, size and movement identification.

Bright lighting can lead to gradual eyesight weakness due to ocular nerve fatigue and effects on the central nervous system. This results in fatigue, lack of efficiency, and higher levels of accidents and injuries especially when there is significant disparity in the lighting within different areas of a workplace. 2- Noise hazard: it is a clashing combination of sounds across the work area. These sounds affect the activeness of workers, resulting in a decrease in productivity along with other long term effects on workers' health and spirit (Abdallah, 2007).

Following are some a number of effects caused by noise hazard:

- Difficulties in communication among workers.
- Psychological effects as unease, depression, and rage.
- Neurological and physiological effects which mainly affect the productivity of workers.

- Lack of concentration and mental abilities which require patience and accuracy.

2- Heat: this is a form of energy which causes increase in amounts of temperature reaching bodies. Its unit of measurement is calorie which equals the amount of temperature needed to raise the heat of one kilogram of water one degree (Taha, 1985).

Exposure to heat can lead to the following:

- Psychological and nervous disorders as unease and rage.
- Painful hand and feet muscle contractions accompanied with vomiting.
- Heat strokes (sun stroke) due to high temperature along with dizziness, tremor and fainting.
- Skin inflammation.
- Eye inflammation including eye lids, and leading to corneal opacity and weak vision.

3- Ventilation: This is a process by which clean air is provided to the workplace and stale air is removed. The aim is to create a suitable environment and work space to achieve better productivity and provide safety for workers (Abdalgani, 2001).

Exhaling stale or polluted air at the work place can result in the following:

- Health conditions as headaches, sleepiness, fatigue, and lack of energy.

- Polluted air can result in worker suffocation.

4- Dust and dirt: These are fine particles of solid matter resulting from mechanical processes as grinding, hammering, filtering and others. Such processes spread particles with properties similar to the original matter in the air (Abdallah, 2007). A work atmosphere saturated with dust and dirt affects workers and their productivity, having the following negative results:

- Workers lose the ability to work efficiently due to limited or blurred vision.
- Cases of collision and falling from high places increase due to dizziness in the head.
- The respiratory system is affected mainly if the dust includes toxic chemical matters.

Mechanisms for improving work conditions

All organizations will have work conditions which affect their workers and thus their productivity. Therefore, the administration works towards bettering these conditions through a number of mechanisms which include:

1- Having the right person for the right job to avoid cases of psychological maladjustment and psychological disorders.

2- Encouraging relations between members of one group and among different groups. This will create an atmosphere of cooperation and fair competition.

3- The workplace need be clean and comfortable regarding lighting and ventilation, and free from noise hazard and dust which affect workers negatively (Alasawi, 1997).

4- The organization is to provide workers with proper accommodation and health care. This will increase their morale, decrease their transport costs, and reduce sickness resulting from terrible social conditions.

5- Assuring services of luxury for workers and their families as this creates a positive worker inside and outside the organization (Hanan, 2006).

6- Taking into consideration the organizational structure and reforming it from time to time.

7- The administration is to adopt a humanist philosophy and care for the human factor and provide support and guidance whenever needed.

8- Dealing with routine and reducing it as much as possible through the application of modern technology.

9- Having clear and consistent organizational policies and being concerned with training and developing worker competencies.

10- Reducing physical burdens of a post through simplifying moves, bettering work positions and reducing the number of tasks allocated to a worker (Alshanti, 2006).

2.9 Job Satisfaction

The term 'job satisfaction' is used to refer to workers' feelings towards their jobs. The matter of job satisfaction and dissatisfaction is the outcome of the relation a worker perceives between the goals s/he aims to gain from his/her job and what is actually expected to be gained from this job, Job satisfaction is concerned with psychological, physical and environmental conditions which lead the worker to say truthfully "I am satisfied with my job" (Aladili, 1981). Shawish (2004) has mentioned that the level of job satisfaction in the light of the above definition represents an implicit individual behavior, which may continue to be implicit, but show in the individual's visible behavior. However, individuals vary in the extend at which their visible behavior reflects their implicit psychological attitudes. Alnamir (1993) perceived job satisfaction as workers' expressions towards their jobs. These feelings are based on two dimensions:

- What workers believe their work will take them to.
- What workers expect to achieve via their jobs.

Researchers have introduced many definitions for the term 'job satisfaction'. Alaghbari (2002) defined job satisfaction as a reflection of the level of balance between positive and negative feelings towards a job with

all its aspects including salary, work conditions, relations with managers and coworkers, promotions and professional growth.

The many definitions of job satisfaction vary, but can be summarized as individuals' feelings and attitudes towards their job which results in a feeling of joy, whilst dissatisfaction leads to unwillingness to work.

According to Abedawi (2006) Job satisfaction is a result of a number of factors related to the facility. These include:

1- Administrative policies in organizing the work and its suitable conditions.

2- Supervision and relations with direct superiors.

3- Coworker relationships.

4- Salary or wages.

5- Promotion opportunities and progress in work.

6- Work privileges within the facility.

7- Safety, security and employment stability.

8- Job responsibilities and their accomplishment.

9- Job status, acknowledgment and appreciation.

10- Working hours and working team.

11- Physical work conditions.

2.10 Conceptual Framework and Hypothesis Development:

Figure 1 shows the conceptual model depicting the five variables. It is submitted according to the conceptualized research model that: Individual Factors of Generations of employees influence their compliance with Information Security policies, Organizational Factors of Generations of employees influence their compliance with Information Security policies, Employees Satisfaction and Technological Work Environment of Generations of employees influence their compliance with Information Security policies, The development of the hypotheses is discussed in the following sections.

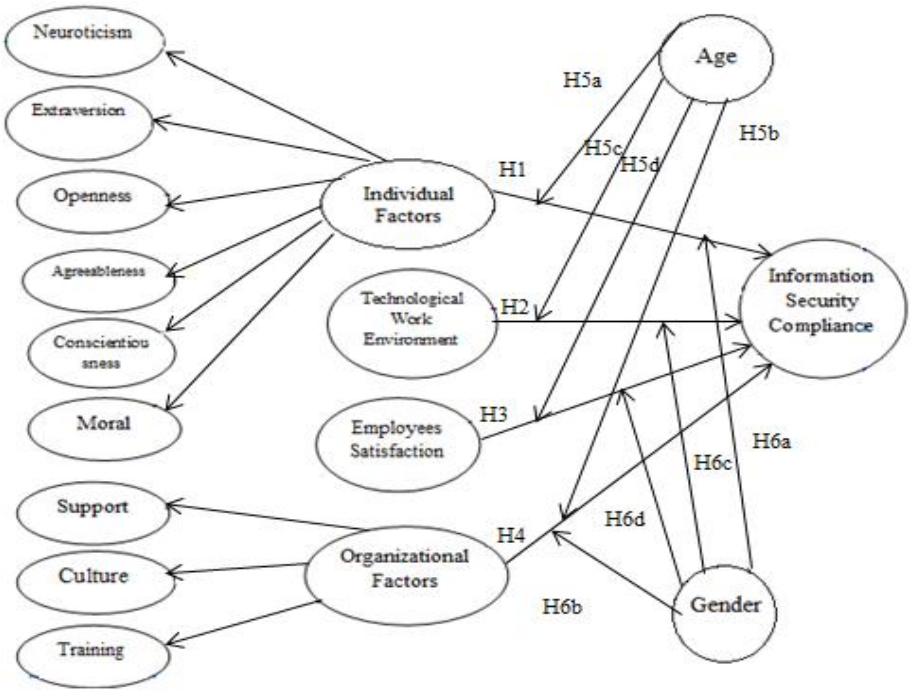


Figure 1: Conceptual framework

2.10.1 Relationship between Individual Factors and Information Security Compliance Policy

The specific and inherent individual employee characteristics linked to security policy compliance are encompassed by dispositional and personality traits. Aspects of an individual's standards of ethics are included in the most salient factors examined in the security policy research. Examples of these are: morality (Myyry et al., 2009; Hu et al., 2011; Vance & Siponen, 2012), personal norms (Ifinedo, 2014), and virtuousness (Siponen & Livari, 2006). There work suggests that either personality or dispositional traits have a direct link to conformity with security policy compliance or that constructs such as attitude mediate this link. Johnston et al. (2016), found that the link between how an employee perceives a situation (e.g., threat vulnerability and sanction severity) and their intention to adhere to a security policy is influenced by dispositional factors such as agreeableness, extraversion, conscientiousness, neuroticism and openness. Bulgurcu et al. (2010), Moquin & Wakefield (2016) and Foth (2016), have established a connection between attitude and policy compliance whereas other work finds a variation in the strength of this connection that varies according to country (Dinev et al., 2009). Further work suggests that there is no convincing link at all (Guo et al., 2011). Thus, we can say that:

H1: Individual Factors influence significantly of employees compliance with Information Security policies.

2.10.2 Relationship between Technological Work Environment and Information Security Compliance Policy

In the operational environment there are many sources of distraction, such as lighting, vibrations, noise and temperature. These can be the cause for error even for an experienced employee if they are not correctly adjusted (Chaula et al., 2006). Therefore it is proposed that:

H2: High Technological Work Environment influence positively of employees compliance with Information Security policies.

2.10.3 Relationship between Employees Satisfaction and Information Security Compliance Policy

The socio-emotional impact of security policies can contribute to how policies are complied with, for example, where positive social and emotional outcomes are generated by a security policy, such as job satisfaction (D'Arcy and Greene, 2014) this has an impact on the employees such that they comply with the guidelines. Contrastingly, stress-inducing security policies (D'Arcy et al., 2014) and ambiguity and conflict in roles (Teh et al., 2015) have been found to lead to non-compliance**.** It is therefore proposed that:

H3: Satisfaction of employees influences positively of employees compliance with Information Security policies.

2.10.4 Relationship between Organizational Factors and Information Security Compliance Policy

The level to which employees comply with a security policy is driven by organizational and managerial characteristics that are included in the culture of information security and support. Some of the characteristics that have a positive influence on compliance with security policy are discussed in the literature. These include climate, organizational values, and norms (Chan et al., 2005; Goo et al., 2014), and awareness, security training, and visibility (Bulgurcu et al., 2010; Lowry et al., 2015; Siponen et al., 2010). Other characteristics, however, produce inconsistent results. For example, managerial support and commitment and was found by much of the literature to have a positive association with compliance (Chan et al., 2005; Herath & Rao, 2009b), but other papers - D'Arcy and Greene (2014) and Ng et al. (2009) - propose that organizational support has either a negative or a negligible impact on security behaviors. This study therefore proposes that:

H4: Organizational Factors influences positively of employees compliance with Information Security policies.

2.10.5 Moderating Effect of age on Information Security Compliance Policies

The moderator is defined by Baron and Kenny (1986) as a variable that affects the strength and/or direction of the association between an independent and a dependent variable. Some research suggests that

differences in age and consistent differences in needs may result in varying reactions in employees to the same HR development practices. The relevance of age in HRM studies is due to its representation of the biological, psychological, and social functioning evolutions (Kooij et al., 2010) that take place in people's lives over time (De Lange et al., 2006; Settersen and Mayer, 1997). There is a lot of evidence to suggest that employees' motivations change over time and with age. Motivational structures in younger and older employees differ and this may be due to changes that occur in individuals over time, varying career situations and organizational rewards, according to Kanfer and Ackerman (2004). Older workers, thus, may focus less than their younger colleagues on training and other forms of development. Ebner et al. (2006) posited that whilst younger individuals' goals were more centered around growth, older individuals' focus was on maintenance. Similarly, in Freund's (2006) research, it was discovered that younger adults were more focused on optimizing performance, whilst older adults focus was rather on minimizing loss. These theories suggest that as they begin to detach from their workplace, developing a self-image that does not rely on career success, older employees are concerned less with development and more with preservation.

The mediating effect of age on the relationship between employee outcomes and HR practices is only focused on in a few studies. In his 2004 paper, Conway examines the relationship between approaches to HR practices and the impact of career stage on commitment, finding a

curvilinear effect. In the meta-analysis conducted by Kooij et al. (2010), a similar curvilinear effect was found between employees' perception of HR practices and the effect of age on their commitment. Regarding practices of HR development the results of studies support the authors' hypothesis that the correlation between training advancement, growth and commitment weakens with age. However, these studies do not support the predictions for job satisfaction, which suggests the need for further research. Although over the past years many companies have begun to tailor more training and development for their more elderly workers (Sterns et al., 2002), there is some evidence to suggest that mature employees are less motivated in general than their younger counterparts to participate in development activities (Colquitt et al., 2000). Whilst younger workers are at the beginning of their careers, more senior employees perceive themselves to have a more limited capacity for growth (Zacher and Frese, 2009). It is thus likely that they don't place much value on the training and development activities the organization invests in. Furthermore, it is often the case that policies within organizations do not encourage the participation of mature employees in training and development (Farr et al., 1998), and line managers often do not support their mature workers who want to acquire knowledge and grow in an adequate way because of the influence of negative stereotypical attitudes towards older people (Leisink and Knies, 2011).

It is therefore proposed that:

H5a: Age moderates the relation between Individual Factors and Information Security Compliance Policies in such a way that the relationship is weaker for older workers compared to younger ones.

H5b: Age moderates the relation between Organizational Factors and Information Security Compliance Policies in such a way that the relationship is weaker for older workers compared to younger ones.

H5c: Age moderates the relation between Technological Work Environment and Information Security Compliance Policies in such a way that the relationship is weaker for older workers compared to younger ones.

H5d: Age moderates the relation between Employees Satisfaction and Information Security Compliance Policies in such a way that the relationship is weaker for older workers compared to younger ones.

2.10.6 Moderating Effect of gender on Information Security Compliance Policies

Hair et al. (2017) classified the moderating relationships to two types. Ones as continuous and others as categorical. A continuous moderating effect exists when the moderating variable is metrically measured whereas a categorical moderating effect is when the moderating variable is categorical, such as gender.

H6a: Gender moderates the relation between Individual Factors and Information Security Compliance Policies.

H6b: Gender moderates the relation between Organizational Factors and Information Security Compliance Policies.

H6c: Gender moderates the relation between Technological Work Environment and Information Security Compliance Policies.

H6d: Gender moderates the relation between Employees Satisfaction and Information Security Compliance Policies.

2.11 Summary

To protect any information in an organization, it is necessary to keep pace with the development and technological progress in the organization. The role of human factors within the sphere of Information Security, occupies greater space in literature owing to its significance in data breaches and compliance with IS policies (Soomro et al., 2016). There exists several empirical studies exhibiting the relationships between the factors of information security policy, deterrence and incentives, attitudes and involvement, training and awareness, and management support (Glaspie and Karwowski, 2017), but there is inadequacy in research findings particularly regarding personality traits age that influence policy compliance (Cram et al., 2017). Hence this research will study the effects of varying personality traits of employees belonging to varying generations, on their ability to comply with IS policies.

Chapter Three

Methodology

3.1 Overview

In this chapter, the research approach, sample identification, data collection and analysis methods are presented. This research aims at studying, explaining and analyzing the factors influencing on Compliance with Information Security Policies in Palestine using a quantitative approach to measure the influence of independent variables (Individual Factors, Organizational Factors, Technological Work Environment and Employees Satisfaction) on dependent variable (compliance).

The reason for selecting the quantitative approach is that this study is deductive in its nature. Saunders et al. (2009) argued that deduction possesses several important features; first, the possibility of explaining causal relationships between variables. Second, controls to allow the testing of hypotheses. Third, concepts have to be operationalized, and the final feature is the generalization. Because of these features, there is a need for a quantitative approach to analyze the collected data. Independent variables in this study are as follows:

1- Individual Factors

2- Organizational Factors

3- Employees Satisfaction

4- Technological Work Environment

Dependent variables is:

5- Compliance with Information Security Policies.

3.2 Nature of the study

This study is an explanatory research. Explanatory studies look for explanations of the nature of certain relationships between the independent variables and the dependent variables. It is a study of a phenomenon in an organized manner to explain the relations between the different variables using statistical methods, and through which we can get to explain the reasons between the variables to reach the cause and effect (Saunders, 2011).

In this study, the researcher tries to explain the relationships between the four pre mentioned independent variables and the dependent variable "Compliance with Information Security Policies", and to assess the effect of each of these variables on the dependent variable.

3.3 Data collection method

In order to collect the necessary data, A questionnaire survey method was used. A questionnaire survey was conducted (see appendix 1 and 2 for English and Arabic version respectively). Questionnaire survey has the advantages of collecting a large amount of data from a large size population, simplicity and speed (Saunders et al., 2009). Oates (2006)

considered the survey that is used to obtain data from a large size population as a systematic and standardized method.

The designed questionnaire used closed questions including Likert scale, nominal, and ordinal in which the respondents can choose from a given set of alternatives. The researcher used a five point Likert scale with anchors defined as (1) strongly disagree , (2) disagree, (3) neutral, (4) agree and (5) strongly agree.

The questionnaire consisted of two main divisions: demographic characteristics and the study factors. Demographic characteristics included gender, age, educational level, social status, job title, specialization, place of residence and work, and "Certificates and years of experience in information security ". On the other hand, the second division consisted of five sections; four sections for each of the four independent variables and the fifth for the dependent variable. The number of questions for each item was 6-10 questions yielding a total of 81 questions which in turn generated a long questionnaire. Despite of the researcher' attempts to reduce this number, none of the questions was excluded as it covered a certain dimension of the procedural definition of the variable. The questionnaire was designed based on the measurements of different scholars available in literature, as shown in Table 2.

Table 1: the references for each item

	Variable' measure	Adopted from
Variable	**1. Individual Factors**	
	a. Neuroticism	
NEUR1	I don't feel afraid nor stressed while working through using a computer.	(Da Raad, 2000; Zhaug, 2006)(
NEUR2	I don't feel that my value is lower than the value of my work colleagues	(DaRaod , 2000),(Zhaug, 2006)
NEUR3	I don't feel that I will have a nervous breakdown while working under a huge pressure	)Bruk& Allen 2003(
NEUR4	I don't feel angry about the way I am treated	(DaRaod, 2000; Zhaug, 2006)
NEUR5	I don't have a pessimistic view towards life	(DaRaod, 2000; Zhaug, 2006; Haward, 1995)
NEUR6	I don't feel sometimes depressed and helpless.	(Costa &Mccrae, 1995)
	b. Extraversion	
EXTRA1	People perceive me as a cheerful, and active person who is full of energy	(Costa &Mccrae, 1995; Haward , 1995)
EXTRA2	I respond to jokes and smile fast	)Costa &Mccrae, 1995(
EXTRA3	I enjoy talking to people	(DaRaod, 2000; Zhaug, 2006)
EXTRA4	I love being friendly and nice with others	)Costa &Mccrae 1995(
EXTRA5	I have a broad social relationship network	)Costa &Mccrae 1995(
EXTRA6	I love going to malls. I like the colors, lights and the crowds at malls.	)Costa &Mccrae 1995(
	c. Openness	
OPEN1	I am keen to illustrate my opinion	(Howard & Howard , 1995)
OPEN2	Using imagination and meditation participates in organizing time	)Alanzi, 2007(
OPEN3	I love travelling and visiting new places	)Costa &Mccrae, 1995(
OPEN4	I see beauty in the things that people perceive as being ordinary	)Alanzi, 2007(
OPEN5	I enjoy reading books and periodicals	)Costa &Mccrae, 1995(
OPEN6	I highly enjoy reading journals, and magazines, and surfing social media websites	(Costa &Mccrae, 1995)
	d. Agreeableness	
AGRE1	I highly believe that my work colleagues have good intentions	(Costa &Mccrae, 1995; DeRaod , 2000; Zhaug, 2006)
AGRE2	I exert much effort in order to meet my goals	(Ewen, 1998)
AGRE3	I help my work colleagues much	(Bruk&Allen 2003; Haward, 1995)
AGRE4	I don't like hurting others' feelings	(DeRaod 2000; Zhaug, 2006)

AGRE5	I carry out my work tasks accurately and efficiently	(Ewen, 1998)
AGRE6	I forgive the ones who did a disservice to me	(Costa &Mccrae, 1995)
	e. Conscientiousness	
CONSC1	I seek organizing my stuff and ensuring that they are clean.	(Costa &Mccrae, 1995)
CONSC2	I seek showing compliance with the institution's bylaw	(Howard & Howard,1995) (Costa &Mccrae, 1995)
CONSC3	I keep working - without stopping - till I finish my work	(Costa &Mccrae, 1995)
CONSC4	If things went bad, I don't feel desperate	(Costa &Mccrae, 1995)
CONSC5	I seek finishing my works before the due time and without receiving help from anyone.	(Costa &Mccrae, 1995)
CONSC6	People depend much on me. They trust me much	(Alanzi, 2007)
	f. Moral	
MOR1	I protect the institution's assets, including the institution's devices and apparatus	(Greenberg, 2002)
MOR2	When there is a problem at work, I exert effort to solve it instantly	(Myyry et al., 2009)
MOR3	I am ready to handle the responsibility for my wrong acts	(Myyry et al., 2009)
MOR4	I highly respect my work colleagues and I don't like talking about them	(Vance &Siponen, 2012)
MOR5	I refrain from disclosing classified information to other institutions	(Myyry et al.,2009)
MOR6	I search for methods and means that can improve my work performance	(Myyry et al., 2009)
	2. Organizational Factors	
	a. Support	
SUPP1	If I faced a problem, I receive support from the institution's management	(Tekleab & Chiaburu, 2011)
SUPP2	If I faced a problem, I receive support from my work colleagues	(Zumrah, 2014)
SUPP3	The institution's management seeks ensuring that the employees understand the goals.	(Tekleab& Chiaburu, 2011)
SUPP4	Periodical reports are delivered about the extent of meeting the goals	(Tekleab&Chiaburu, 2011)
SUPP5	I feel that my contribution to the institution are valuable and significant	(Tekleab**&**Chiaburu, 2011; Singh & Malhotra, 2015)
SUPP6	I receive adequate attention from the institution's management	(Eisenberger, 1990; George, 1999)
	b. Training	
TRAIN1	I am provided with the needed training that enables me to meet my professional needs	(Altaani, 2007)

TRAIN2	I receive the needed training about the information security policies	(Altaani, 2007)
TRAIN3	The training I receive enables me to improve my professional skills	(Alshawani, 2003)
TRAIN4	The institution's management provides employees with training regularly	(Salah, 2004)
TRAIN5	I receive theoretical and practical training	(Alshawani, 2003)
TRAIN6	I receive training courses that suit my institutional position	(Altaani,2007)
	c. Culture	
CULT1	My institution provides much attention to the aspects related to the employee's personality. That is because the institution's management believes that all the employees are a big family	(Al-Qaruiti, 2000)
CULT2	The institution's management seeks establishing an innovative culture	(Edgar, 1986)
CULT3	The institutional culture of my institution participates in building stable relationships between employees	(Al-Qaruiti, 2000)
CULT4	The institution's management of my institution encourages employees to excel at work	(Al-Qaruiti, 2000)
CULT5	The institutional culture of my institution participates in meeting the goals and raising productivity	(Al-Qaruiti, 2000)
CULT6	The institution's management of my institution seeks developing human resources	(Al-Qaruiti, 2000)
	3. Employees Satisfaction	
SATISF1	I am satisfied with my current basic salary when comparing it with the amount of tasks and responsibilities that I must handle	(Alakhbari, 2002; Aladeli, 1981)
SATISF2	My job security level in the institution I work at is high	(Aladili, 1981)
SATISF3	My direct supervisor deals in a fair manner with me	(Alakhbari, 2002; Aladili, 1981)
SATISF4	The moral incentives that I receive from my direct supervisor increase my productivity	(Alakhbari, 2002**;** Aladili, 1981)
SATISF5	I go in a bad mood in case I committed a fault that represents noncompliance with the institution's policies	(Shawish, 2004; Landy&Trumbo, 1980; Aladili, 1981)
SATISF6	I highly believe that the institution I work at retains the outstanding employees	(Alakhbari, 2002)
	4. Technological Work Environment	
TECH1	The institution has programs for	**(**Feleh& AbdelMajeed, 2009)

	protecting all its devices. These programs uploaded in a regular manner	
TECH2	The institution's communication channels are characterized with transferring information smoothly	(Saed, 1987; Alkbasi & Amer, 1998; Feleh& AbdelMajeed, 2009)
TECH3	The workplace is well-lit	(Alaswai, 1997; Bilal, 2011; Owadah, 1996)
TECH4	The workplace includes office supplies and great decorations	(Alaswai, 1997; Hanan, 2006)
TECH5	There are modern and advanced devices at the workplace	(Hanan, 2006; Feleh& AbdelMajeed, 2009)
TECH6	The availability of air condition devices in my office enables me to focus in work	(Alaswai, 1997; Taha, 1985; Algani, 2001; Ali, 2010; Feleh& AbdelMajeed, 2009; Owadah, 1996)
TECH7	The workplace is characterized with being far away from the city center and noise	(Alaswai, 1997; Owadah, 1996)
	5. Information Security Compliance Policies	
COMP1	I believe that practicing my profession requires acknowledging the institution's bylaws, regulations, and instructions.	(Chang & Ho, 2006; Albrechtsen & Hovden, 2010; Kwon et al., 2012)
COMP2	The policies and procedures related to information access are clear	(Loster, 2005; Albrechtsen & Hovden, 2010)
COMP3	All the employees acknowledge the information security policy. There has been an agreement reached on the latter policy	(Loster, 2005; Albrechtsen&Hovden, 2010)
COMP4	The password that I use consists from a mixture of words, numbers, and letters	(Sui et al., 2012; Line et al., 2011)
COMP5	When going on a break or to the bathroom, I shut down my computer	(Albrechtsen, 2007; Line et al., 2011)
COMP6	I don't download files from websites that are not well-known	(Albrechtsen, 2007; Line et al., 2011).
COMP7	I instantly report any bug gets detected in the system	(Albrechtsen, 2007; Line et al., 2011)
COMP8	I protect my personal information. I consider protecting such information as something important	(Harkins, 2012)
COMP9	When using my institution's devices, I don't use a wireless network of any other institution	(AL-Mayahi & Sa'ad, 2014)
COMP10	I make backup copies for the important files	(AL-Mayahi&Sa'ad.2014; Stewart et al.,2012)
COMP11	I don't use the social network websites while working	
NEUR :Neuroticism, EXTRA: Extraversion, OPEN : Openness, AGRE: Agreeableness, CONSC: Conscientiousness, MOR : Moral, SUPP : Support , TRAIN : Training, CULT: Culture, SATISF : Satisfaction, TECH : Technological , COMP : Compliance		

The questionnaire was distributed in a paper questionnaire forms through various provinces in different type of companies. Different means were used to distribute the paper questionnaire including contact with mangers in different companies then they distributed the questionnaire to their employees, and personal contact with employees in the different areas.

The researcher distributed about 500 copies of the paper questionnaire. 372 usable questionnaires were retrieved for the final data analysis, representing a response rate of 74 per cent. This rate would have been higher if the questionnaire was shorter. Some respondents complained about the length of the questionnaire, others apologized for not having time to fill the questionnaire. Out of this number, 46 questionnaires have been excluded because they were invalid.

3.4 Generations X and Y

It is wiser to segregate the individuals under study based on the generations they belong to, since an organization always has people from varying age groups. Generation X refers to those born within the period 1960-1980. They are often referred to as the Nomad generation, a typical example of the Lost Generation of 1890s and 1900s. Both these generations share a general disdain and disaffected attitude towards everything they encountered. The X's hated the generation ahead of them (Boomers) and transformed in every way possible, right from music to politics. As individuals, Generation X has a reputation for being cynical and nihilistic, and this certainly is understandable owing to the several times of economic

crisis, cold war, limited financial aids, AIDS epidemic, etc., that they had to survive amongst. These nomads could have been outrageous as youths but have now moved into the more matured middle age with a better sense of reliability and responsibility. Leaders from Generation X are sensible, cunning, and pragmatic and cannot be fooled very easily. Generation Y refers to the ones born within the years 1980-2000. They are commonly referred to as the millennial generation, a typical example of the honorable Hero Generation who fought World War-II. The Y's have had a charmed life and since their parents did have access to birth-control, they were usually wanted and nurtured children. Their families were highly stable and were sheltered better by the society, in comparison with their predecessors. They are also called the Peter Pan Generation, since they had a great childhood and thus would prefer to delay adult life. However, they are comparatively more orthodox than the Nomads in their approaches, and as policy makers they are downright conventional. Also the Millennial wouldn't blame past events for something like global recession or climate change but seeks for better solutions for the future. On a concise note, Generation X are the ones who will tear down like they did with the establishments of the Boomers while Generation Y will have no issues in rebuilding and sustaining them. While Generation X are the best educated, technologically savvy trying to leverage technology for humanizing and personalizing everything, Generation Y are more optimistic, less cynical, better at multitasking, more tech savvy and comfortable in adopting latest tools and technology, etc., in comparison (Halsall, 2017; Reisenwitz et al., 2009; Lissitsa & Kol, 2016).

3.5 Study Population

The target population for the study was Palestinian employees in Palestine who work with computer. The sampling unit was the employee who uses a computer in his work. The study sample will be selected randomly from employees in various provinces at different type of companies.

The largest companies and organizations in Palestine have been selected. Universities, telecommunications and Internet companies, insurance companies and banks were selected. Table 1 shows the organizations was sampled.

Table 2: Organizations was sampled

NO.	Organizations	NO. Of Employees	NO. Of Sample	NO. Of Responses
1	Arab American University	700	50	30
2	An-Najah National University	2000	170	138
3	Birzeit University	700	80	68
5	Paltel Company	1000	20	13
6	Jawwal Company	800	20	16
8	Super link company	30	15	13
9	Mada Company	35	20	13
11	Bank Of Palestine	1000	20	14
12	Alsafa Bank	30	20	13
13	Islamic Bank of Palestine	400	20	15
14	Arab Bank	1000	10	5
15	AL-Takaful Insurance	150	20	12
16	National Insurance Company	150	15	9
17	Global Insurance	150	20	13
	Total	**8145**	**500**	**372**

In order to determine the required sample size three elements should be identified first:

1- Population size: the size of the whole population.

2- Confidence level: the level of certainty that the gathered sample characteristics represent the population characteristics.

3- Confidence interval (precision level): the margin of error that can be tolerated.

In the current study, a confidence level of 95% is chosen, and a confidence interval of 5 (error margin is 0.05) is selected.

3.6 Study Sample Calculations

The required sample size needed to be drawn from this population so that the results could be generalized on the population at a level of confidence of 95%, and error margin of 5% can be calculated using equation adopted from Daniel and Cross (2013):

$$n = \frac{Nz^2pq}{d^2(N-1)+z^2pq}$$

Where:

n: is the sample size

N: is the population size

Z= 1.96 corresponding to a 95% confidence level

p is the percentage picking a choice from the population, when p=0.5 the largest possible sample size is produced.

q=1-p=0.5

d is the acceptable error margin (5%).

$$n = \frac{8145 * 1.96^2 * 0.5 * 0.5}{0.05^2 * (8145 - 1) + 1.96^2 * 0.5 * 0.5} \approx 367$$

Substituting all of these values in the equation yields n = 367. Therefore, based on these values, the researcher has to collect at least 367 survey items so that the results can be generalized on the population.

3.7 Data Analysis Method

This study used Smart PLS v3.2.7 software for the Structural Equation Modeling (SEM) technique in order to carry out a statistical analysis of the measurement and structural models (Ringle et al., 2005). The measurement model in SEM relates to the connections between the latent variables and their manifest variables. The structural model refers to the hypothesized causal relationships between the research constructs (Chin & Newsted, 1999). The simultaneous investigation in one model of both the path (structural) and factor (measurement) models is enabled by SEM. In addition to this, the Smart PLS software makes only minimal assumptions and combines a factor analysis with near regressions with the goal of variance in explanation (high R- square) (Chin, 1998). Furthermore, Smart

PLS enables both confirmatory and exploratory research, is robust enough to cope with deviations in multivariate normal distributions, and is ideal for large sample sizes. Smart PLS was found to be more appropriate for the purposes of the current study as the current sample size of the study is relatively large (372).

3.8 Reliability and validity

Reliability and validity were among the goals of the research while collecting the required data.

3.8.1 Reliability

A model for measuring the conceptual model was deduced using five latent variables. Reflective indicators were used to model all constructs because in the earlier study, this same method was used. Composite Reliabilities (CR) values and Cronbach's Alpha (CA) values were used to assess the reliability of the construct reliability and, as indicated in Table 3, the values of CR and the CA meet Hulland's (1999) recommendations of all being above 0.6. According to Hulland,(1999) , any value that is above 0.4 won't be rejected in case of the exploratory research . As a result of the values for composite reliability ranging from 0.847 to 0.950 and from 0.772 to 0.939 for all of Cronbach's alphas, the conclusion is here drawn that the scales are reliable.

Table 3: Statistics Regarding Accuracy Analysis

Constructs	Items	Loading	AVE	CR	CA
Individual Factors					
Neuroticism	NEUR1	0.614	0.513	0.862	0.810
	NEUR2	0.617			
	NEUR3	0.770			
	NEUR4	0.755			
	NEUR5	0.764			
	NEUR6	0.758			
Extraversion	EXTRA1	0.786	0.556	0.862	0.801
	EXTRA2	0.771			
	EXTRA3	0.773			
	EXTRA4	0.748			
	EXTRA5	0.702			
Openness	OPEN1	0.598	0.566	0.885	0.854
	OPEN2	0.796			
	OPEN3	0.830			
	OPEN4	0.868			
	OPEN5	0.678			
	OPEN6	0.710			
Agreeableness	AGRE2	0.883	0.566	0.885	0.854
	AGRE3	0.558			
	AGRE4	0.584			
	AGRE5	0.728			
	AGRE6	0.874			
Conscientiousness	CONS1	0.706	0.527	0.847	0.772
	CONS2	0.776			
	CONS3	0.781			
	CONS5	0.745			
	CONS6	0.608			
Moral	MOR1	0.804	0.509	0.860	0.804
	MOR2	0.743			
	MOR3	0.756			
	MOR4	0.610			
	MOR5	0.730			
	MOR6	0.613			
Organizational Factors					
Support	SUPP1	0.797	0.528	0.867	0.815
	SUPP2	0.586			
	SUPP3	0.854			
	SUPP4	0.682			
	SUPP5	0.560			
	SUPP6	0.825			
Training	TRAIN1	0.872	0.702	0.933	0.912
	TRAIN2	0.833			
	TRAIN3	0.608			
	TRAIN4	0.865			
	TRAIN5	0.900			
	TRAIN6	0.913			
Culture	CULT1	0.850	0.767	0.950	0.939

	CULT2	0.893			
	CULT3	0.875			
	CULT4	0.888			
	CULT5	0.914			
	CULT6	0.832			
Employees Satisfaction	SATISF1	0.615	0.521	0.866	0.820
	SATISF2	0.735			
	SATISF3	0.751			
	SATISF4	0.680			
	SATISF5	0.809			
	SATISF6	0.726			
Technological Work Environment	TECH1	0.701	0.504	0.876	0.834
	TECH2	0.635			
	TECH3	0.780			
	TECH4	0.768			
	TECH5	0.800			
	TECH6	0.692			
	TECH7	0.565			
Information Security Compliance Policies	COMP1	0.719	0.508	0.911	0.891
	COMP2	0.674			
	COMP3	0.616			
	COMP4	0.694			
	COMP5	0.731			
	COMP6	0.617			
	COMP7	0.811			
	COMP8	0.765			
	COMP9	0.804			
	COMP10	0.661			

Four questions were deleted from several different factors because they did not match reliability. By deleting a question for each of these four factors, a question was removed from each of the Extraversion, Agreeableness, Conscientiousness and "Information Security Compliance Policies".

Convergent validity, also known as internal consistency, has been assessed using the measure of average variance extracted (AVE) and the factor item loading values. Fornell and Lacker’s (1981) suggested that the criteria should be 0.5, and, as is observed in Table 3, all the AVE values and the item loadings conform to the suggested criteria. This confirms the existence

of convergent validity due to its implication that all the items converged on the construct they were meant to be measuring.

3.8.2 Validity

Joppe (2000) defined validity in quantitative research as whether the research instrument measures what it is intended to be measuring. In this research, the validity was tested by showing the questionnaire to four different arbitrators (see appendix who evaluated the survey items, the judges' comments were taken into consideration through the process of designing the survey). In addition, most of the measures used in the questionnaire were adopted from previous studies available in literature which in turn used them and proved their validity, therefore the current measures are considered valid.

The AVE of a variable that is latent must be greater than the correlations between the latent variable and all the other variables squared in order to assess its discriminant validity (Fornell & Larcker, 1981; Chin, 2010). In Table 4 the correlation matrix is listed with correlation between the constructs and the square root AVE on the diagonal (Chin, 1998).

Note: AG = Agreeableness; CO = Conscientiousness; CU = Culture; ES = Employees Satisfaction; EX = Extraversion; ISP = Information Security Compliance Policies; MO = Moral; NE = Neuroticism; OP = Openness; TWE = Technological Work Environment; TR = Training; SU = Support.

Table 4: Inter-Construct Correlations and Shared Variance

	AG	CO	CU	ES	EX	ISP	MO	NE	OP	SU	TWE	TR
AG	**0.737**											
CO	0.316	**0.726**										
CU	-0.003	0.146	**0.876**									
ES	0.094	0.183	0.601	**0.722**								
EX	0.221	0.342	0.154	0.122	**0.746**							
ISP	0.041	0.407	0.346	0.223	0.244	**0.712**						
MO	0.195	0.605	0.102	0.175	0.296	0.509	**0.713**					
NE	0.104	0.267	0.242	0.217	0.306	0.340	0.348	**0.716**				
OP	0.053	0.031	0.086	0.091	0.079	0.064	0.036	0.112	**0.752**			
SU	0.068	0.269	0.722	0.718	0.239	0.385	0.209	0.331	0.133	**0.727**		
TWE	-0.098	0.203	0.562	0.434	0.206	0.567	0.229	0.367	0.127	0.603	**0.710**	
TR	-0.042	0.089	0.746	0.562	0.106	0.298	0.051	0.186	0.113	0.692	0.525	**0.838**

Table 5 demonstrates that the off diagonal elements are smaller than the diagonal elements in the corresponding rows and columns confirming thus that discriminant validity does indeed exist. An indicator should have a higher loading on its assigned latent variable on all other latent variables (Fornell & Larcker, 1981).

As stated by Chin (1998), cross-loading is obtained by correlating each latent variable's component scores with all of the other items. If each indicator's loading is higher for its designated construct compared to any other constructs, then it can be inferred that the different constructs' indicators are not interchangeable.

Therefore, the item's loading of each indicator is highest for its designated construct.

Note: Ag = Agreeableness; Co = Conscientiousness; Cu = Culture; ES = Employees Satisfaction; Ex = Extraversion; ISP = Information Security Compliance Policies; Mo = Moral; Ne = Neuroticism; Op = Openness; TWE = Technological Work Environment; Tr = Training; Su = Support.

Table 5: list the Cross Loading

	Ag	Co	Cu	ES	Ex	ISP	Mo	Ne	Op	Su	TWE	Tr
Ag2	0.883	0.317	0.045	0.065	0.222	0.065	0.179	0.102	0.097	0.079	-0.077	-0.009
Ag2	0.883	0.317	0.045	0.065	0.222	0.065	0.179	0.102	0.097	0.079	-0.077	-0.009
Ag3	0.558	0.146	-0.081	0.066	0.023	0.021	0.116	0.021	-0.017	0.009	-0.034	-0.040
Ag3	0.558	0.146	-0.081	0.066	0.023	0.021	0.116	0.021	-0.017	0.009	-0.034	-0.040
Ag4	0.584	0.110	-0.097	0.075	0.095	-0.004	0.143	0.106	0.083	0.011	-0.106	-0.085
Ag4	0.584	0.110	-0.097	0.075	0.095	-0.004	0.143	0.106	0.083	0.011	-0.106	-0.085
Ag5	0.723	0.255	-0.006	0.083	0.169	0.028	0.139	0.049	-0.094	0.043	-0.066	-0.070
Ag5	0.723	0.255	-0.006	0.083	0.169	0.028	0.139	0.049	-0.094	0.043	-0.066	-0.070
Ag6	0.874	0.276	0.050	0.068	0.231	0.024	0.144	0.094	0.093	0.078	-0.080	0.013
Ag6	0.874	0.276	0.050	0.068	0.231	0.024	0.144	0.094	0.093	0.078	-0.080	0.013
Com1	0.092	0.266	0.222	0.200	0.090	0.719	0.343	0.219	0.049	0.312	0.399	0.198
Com10	0.053	0.308	0.145	0.029	0.154	0.661	0.340	0.120	-0.013	0.090	0.287	0.165
Com2	0.044	0.293	0.384	0.315	0.155	0.674	0.378	0.301	0.028	0.445	0.522	0.320
Com3	-0.015	0.232	0.508	0.308	0.145	0.616	0.241	0.265	0.063	0.534	0.534	0.423
Com4	0.069	0.358	0.205	0.107	0.200	0.694	0.390	0.269	0.030	0.241	0.351	0.159
Com5	0.001	0.280	0.215	0.117	0.178	0.731	0.355	0.239	0.072	0.229	0.350	0.203
Com6	-0.020	0.216	0.058	-0.009	0.128	0.617	0.253	0.091	0.061	0.078	0.227	0.101
Com7	-0.023	0.270	0.221	0.129	0.185	0.811	0.401	0.308	0.054	0.239	0.438	0.181
Com8	0.090	0.386	0.165	0.145	0.281	0.765	0.496	0.238	0.020	0.195	0.381	0.093
Com9	-0.007	0.268	0.217	0.131	0.191	0.804	0.385	0.281	0.091	0.238	0.430	0.204
Con1	0.147	0.706	0.087	0.102	0.212	0.338	0.410	0.125	0.010	0.202	0.225	0.109
Con1	0.147	0.706	0.087	0.102	0.212	0.338	0.410	0.125	0.010	0.202	0.225	0.109
Con2	0.217	0.776	0.082	0.144	0.272	0.337	0.402	0.178	0.043	0.177	0.169	0.032
Con2	0.217	0.776	0.082	0.144	0.272	0.337	0.402	0.178	0.043	0.177	0.169	0.032
Con3	0.242	0.781	0.158	0.159	0.271	0.320	0.484	0.212	0.060	0.231	0.150	0.105

Con3	0.242	0.781	0.158	0.159	0.271	0.320	0.484	0.212	0.060	0.231	0.150	0.105
Con5	0.309	0.745	0.189	0.198	0.207	0.286	0.495	0.229	0.001	0.256	0.123	0.102
Con5	0.309	0.745	0.189	0.198	0.207	0.286	0.495	0.229	0.001	0.256	0.123	0.102
Con6	0.221	0.608	-0.007	0.045	0.281	0.192	0.397	0.218	-0.009	0.096	0.069	-0.037
Con6	0.221	0.608	-0.007	0.045	0.281	0.192	0.397	0.218	-0.009	0.096	0.069	-0.037
Cu1	0.009	0.116	0.850	0.526	0.128	0.295	0.040	0.152	0.032	0.685	0.517	0.677
Cu1	0.009	0.116	0.850	0.526	0.128	0.295	0.040	0.152	0.032	0.685	0.517	0.677
Cu2	0.068	0.146	0.893	0.528	0.125	0.253	0.073	0.170	0.089	0.701	0.418	0.657
Cu2	0.068	0.146	0.893	0.528	0.125	0.253	0.073	0.170	0.089	0.701	0.418	0.657
Cu3	0.012	0.114	0.875	0.540	0.152	0.338	0.100	0.259	0.073	0.710	0.514	0.638
Cu3	0.012	0.114	0.875	0.540	0.152	0.338	0.100	0.259	0.073	0.710	0.514	0.638
Cu4	-0.087	0.074	0.888	0.536	0.071	0.295	0.077	0.171	0.052	0.686	0.451	0.631
Cu4	-0.087	0.074	0.888	0.536	0.071	0.295	0.077	0.171	0.052	0.686	0.451	0.631
Cu5	-0.048	0.143	0.914	0.551	0.159	0.340	0.148	0.249	0.068	0.703	0.557	0.667
Cu5	-0.048	0.143	0.914	0.551	0.159	0.340	0.148	0.249	0.068	0.703	0.557	0.667
Cu6	0.030	0.172	0.832	0.477	0.177	0.297	0.096	0.273	0.140	0.676	0.497	0.647
Cu6	0.030	0.172	0.832	0.477	0.177	0.297	0.096	0.273	0.140	0.676	0.497	0.647
Ex1	0.194	0.219	0.148	0.107	0.736	0.158	0.233	0.341	0.007	0.214	0.125	0.075
Ex1	0.194	0.219	0.148	0.107	0.736	0.158	0.233	0.341	0.007	0.214	0.125	0.075
Ex2	0.105	0.158	0.119	0.095	0.771	0.159	0.139	0.231	0.071	0.176	0.191	0.121
Ex2	0.105	0.158	0.119	0.095	0.771	0.159	0.139	0.231	0.071	0.176	0.191	0.121
Ex3	0.094	0.236	0.114	0.067	0.773	0.206	0.206	0.222	0.111	0.171	0.198	0.098
Ex3	0.094	0.236	0.114	0.067	0.773	0.206	0.206	0.222	0.111	0.171	0.198	0.098
Ex4	0.201	0.312	0.100	0.128	0.746	0.210	0.270	0.168	0.048	0.174	0.134	0.090
Ex4	0.201	0.312	0.100	0.128	0.746	0.210	0.270	0.168	0.048	0.174	0.134	0.090
Ex5	0.210	0.319	0.097	0.054	0.702	0.168	0.235	0.189	0.063	0.155	0.128	0.019
Ex5	0.210	0.319	0.097	0.054	0.702	0.168	0.235	0.189	0.063	0.155	0.128	0.019
Mo1	0.196	0.510	-0.003	0.126	0.263	0.402	0.804	0.270	-0.023	0.117	0.150	-0.044

Mo1	0.196	0.510	-0.003	0.126	0.263	0.402	0.804	0.270	-0.023	0.117	0.150	-0.044
Mo2	0.093	0.456	0.038	0.080	0.228	0.362	0.743	0.252	0.035	0.108	0.120	-0.016
Mo2	0.093	0.456	0.038	0.080	0.228	0.362	0.743	0.252	0.035	0.108	0.120	-0.016
Mo3	0.115	0.484	0.039	0.113	0.241	0.358	0.756	0.242	0.119	0.124	0.159	0.026
Mo3	0.115	0.484	0.039	0.113	0.241	0.358	0.756	0.242	0.119	0.124	0.159	0.026
Mo4	0.156	0.311	0.184	0.169	0.158	0.285	0.610	0.282	0.062	0.210	0.175	0.140
Mo4	0.156	0.311	0.184	0.169	0.158	0.285	0.610	0.282	0.062	0.210	0.175	0.140
Mo5	0.145	0.405	0.081	0.147	0.167	0.395	0.730	0.227	-0.023	0.146	0.171	0.016
Mo5	0.145	0.405	0.081	0.147	0.167	0.395	0.730	0.227	-0.023	0.146	0.171	0.016
Mo6	0.132	0.396	0.144	0.130	0.195	0.374	0.613	0.225	-0.012	0.222	0.222	0.143
Mo6	0.132	0.396	0.144	0.130	0.195	0.374	0.613	0.225	-0.012	0.222	0.222	0.143
Ne1	-0.071	0.119	0.204	0.072	0.171	0.268	0.253	0.614	0.016	0.185	0.266	0.129
Ne2	-0.035	0.141	0.147	0.062	0.178	0.324	0.266	0.617	0.066	0.213	0.370	0.108
Ne3	0.025	0.213	0.093	0.115	0.259	0.267	0.265	0.770	0.046	0.213	0.268	0.078
Ne4	0.131	0.242	0.294	0.294	0.174	0.297	0.253	0.755	0.078	0.370	0.357	0.216
Ne5	0.214	0.211	0.167	0.141	0.282	0.174	0.238	0.764	0.123	0.191	0.158	0.131
Ne6	0.096	0.193	0.149	0.209	0.232	0.179	0.242	0.758	0.129	0.248	0.211	0.135
Op1	-0.031	-0.054	0.215	0.102	-0.001	0.109	-0.037	0.095	0.598	0.220	0.230	0.169
Op1	-0.031	-0.054	0.215	0.102	-0.001	0.109	-0.037	0.095	0.598	0.220	0.230	0.169
Op2	0.027	0.036	0.156	0.109	0.022	0.104	0.066	0.099	0.796	0.155	0.219	0.129
Op2	0.027	0.036	0.156	0.109	0.022	0.104	0.066	0.099	0.796	0.155	0.219	0.129
Op3	0.071	0.025	-0.019	0.028	0.106	0.004	0.016	0.058	0.830	0.026	0.004	0.002
Op3	0.071	0.025	-0.019	0.028	0.106	0.004	0.016	0.058	0.830	0.026	0.004	0.002
Op4	0.085	0.017	0.033	0.069	0.078	0.036	0.038	0.095	0.868	0.074	0.073	0.063
Op4	0.085	0.017	0.033	0.069	0.078	0.036	0.038	0.095	0.868	0.074	0.073	0.063
Op5	-0.029	0.020	0.107	0.071	0.039	0.042	0.029	0.121	0.678	0.154	0.095	0.154
Op5	-0.029	0.020	0.107	0.071	0.039	0.042	0.029	0.121	0.678	0.154	0.095	0.154
Op6	0.023	0.028	0.081	0.087	0.058	0.071	-0.015	0.078	0.710	0.143	0.113	0.135

Op6	0.023	0.028	0.081	0.087	0.058	0.071	-0.015	0.078	0.710	0.143	0.113	0.135
Sa1	0.119	0.071	0.446	0.615	0.024	0.066	-0.009	0.122	0.047	0.463	0.313	0.420
Sa2	0.086	0.095	0.427	0.735	0.094	0.162	0.115	0.221	0.032	0.502	0.310	0.436
Sa3	0.056	0.180	0.373	0.751	0.085	0.128	0.149	0.114	0.068	0.480	0.294	0.359
Sa4	0.196	0.152	0.365	0.680	0.051	0.135	0.143	0.055	0.064	0.436	0.240	0.371
Sa5	0.044	0.147	0.370	0.809	0.050	0.226	0.139	0.148	0.088	0.560	0.348	0.356
Sa5	0.044	0.147	0.370	0.809	0.050	0.226	0.139	0.148	0.088	0.560	0.348	0.356
Sa5	0.044	0.147	0.370	0.809	0.050	0.226	0.139	0.148	0.088	0.560	0.348	0.356
Sa6	-0.022	0.133	0.665	0.726	0.196	0.175	0.156	0.246	0.081	0.666	0.377	0.539
Su1	-0.015	0.181	0.659	0.526	0.144	0.304	0.127	0.225	0.072	0.797	0.453	0.519
Su1	-0.015	0.181	0.659	0.526	0.144	0.304	0.127	0.225	0.072	0.797	0.453	0.519
Su2	0.120	0.226	0.365	0.268	0.243	0.289	0.223	0.289	0.040	0.586	0.387	0.267
Su2	0.120	0.226	0.365	0.268	0.243	0.289	0.223	0.289	0.040	0.586	0.387	0.267
Su3	0.062	0.259	0.678	0.536	0.235	0.281	0.160	0.293	0.117	0.854	0.515	0.566
Su3	0.062	0.259	0.678	0.536	0.235	0.281	0.160	0.293	0.117	0.854	0.515	0.566
Su4	0.083	0.211	0.510	0.399	0.171	0.251	0.153	0.229	0.138	0.682	0.401	0.526
Su4	0.083	0.211	0.510	0.399	0.171	0.251	0.153	0.229	0.138	0.682	0.401	0.526
Su6	0.042	0.170	0.745	0.642	0.195	0.335	0.151	0.266	0.113	0.825	0.507	0.672
Su6	0.042	0.170	0.745	0.642	0.195	0.335	0.151	0.266	0.113	0.825	0.507	0.672
Tech1	-0.062	0.159	0.379	0.227	0.188	0.405	0.124	0.214	0.093	0.411	0.701	0.350
Tech2	-0.021	0.138	0.481	0.291	0.109	0.339	0.089	0.244	0.212	0.460	0.635	0.400
Tech3	-0.014	0.261	0.394	0.343	0.243	0.489	0.290	0.312	0.048	0.429	0.780	0.337
Tech4	-0.052	0.135	0.549	0.436	0.174	0.317	0.078	0.289	0.104	0.576	0.768	0.493
Tech5	-0.078	0.138	0.393	0.375	0.183	0.480	0.220	0.258	0.042	0.449	0.800	0.397
Tech6	-0.240	0.055	0.346	0.246	0.020	0.420	0.132	0.254	0.082	0.382	0.692	0.351
Tech7	0.005	0.094	0.299	0.249	0.075	0.298	0.139	0.262	0.097	0.319	0.565	0.320
Tr1	-0.007	0.088	0.655	0.521	0.157	0.249	0.063	0.217	0.126	0.649	0.419	0.872
Tr1	-0.007	0.088	0.655	0.521	0.157	0.249	0.063	0.217	0.126	0.649	0.419	0.872

Tr2	-0.022	0.108	0.595	0.438	0.076	0.242	0.065	0.219	0.089	0.556	0.446	0.833
Tr2	-0.022	0.108	0.595	0.438	0.076	0.242	0.065	0.219	0.089	0.556	0.446	0.833
Tr3	-0.047	0.184	0.429	0.311	0.021	0.368	0.194	0.172	0.127	0.434	0.387	0.608
Tr3	-0.047	0.184	0.429	0.311	0.021	0.368	0.194	0.172	0.127	0.434	0.387	0.608
Tr4	-0.071	0.025	0.690	0.502	0.083	0.224	0.016	0.129	0.079	0.607	0.443	0.865
Tr4	-0.071	0.025	0.690	0.502	0.083	0.224	0.016	0.129	0.079	0.607	0.443	0.865
Tr5	-0.068	0.027	0.679	0.489	0.078	0.231	-0.017	0.091	0.055	0.595	0.470	0.900
Tr5	-0.068	0.027	0.679	0.489	0.078	0.231	-0.017	0.091	0.055	0.595	0.470	0.900
Tr6	0.001	0.058	0.664	0.529	0.097	0.230	-0.012	0.124	0.105	0.615	0.476	0.913
Tr6	0.001	0.058	0.664	0.529	0.097	0.230	-0.012	0.124	0.105	0.615	0.476	0.913

Chapter Four

Data Analysis and Discussion

4.1 Overview

This chapter presents the analysis of the gathered data in addition to discussing these results. The analysis starts with sample characteristics which are classified into three categories: demographic, Survey items' results and Evaluating Moderating Effects (Age and Gender).

4.2 Sample Characteristics

4.2.1 Demographic characteristics

The respondents identities have been kept anonymous, as no coding have been used. Seven demographic characteristics were considered in the study: gender, age, educational level, social status, job title and years of experience in information security ". According to Halsall (2017), Age was classified into three categories (18-38 Y, 39-58 Y and more than 59 years). As a generation X, and Y. On the other hand, educational level included (less than high school, high school, diploma, bachelor, and higher education). The marital status was either single or married. Regarding to job title was classified as (Manager, Head of the Department, Supervisor, IT Employee, Employee and others). Finally, experience in information security was classified as (less than ten years, 11-20 years, more than 21 years).

Out of the three hundred and seventy two valid surveys, there were 183 (49.2%) males and 189 (50.8%) females. Regarding age, the distribution of employees was as illustrated in Figure 2. The large number of employees according to age was in the age category of 18-38 years with 266 employees, forming 71.5% of the employees, and the small age category was for the employees aged more than 38 years with 106 employees (28.5%).

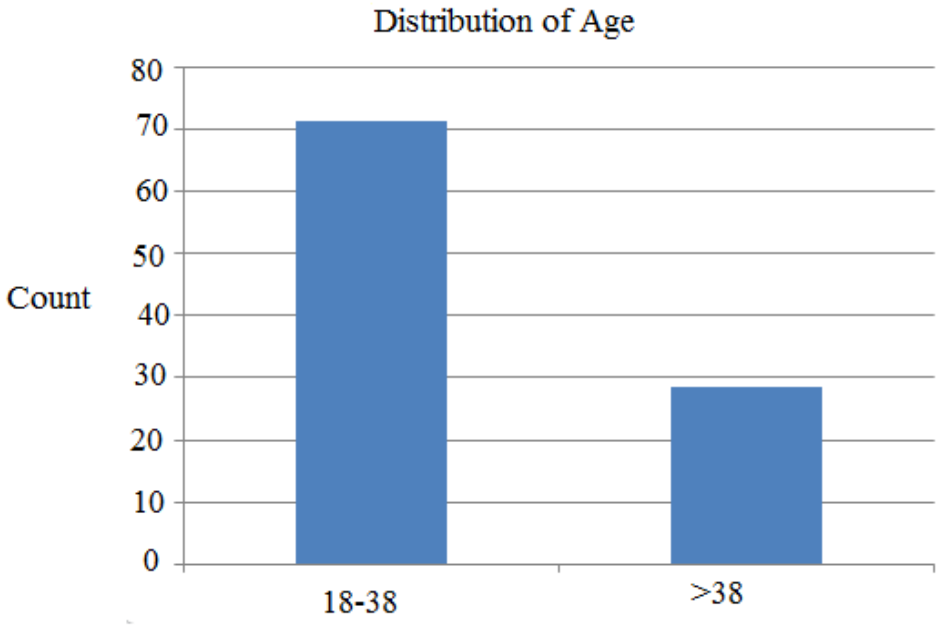


Figure 2: Respondents distribution according to age

On the other hand, relating education the bachelor degree holders were the largest sector with 197 employees (52.95%), next was the category of employees with higher education certificate of 119 employees (32%), followed by diploma holders with 56 employees (15.05%), and finally there is no employees with high school degree and less than high school degree (0%). Figure 3 illustrates these results.

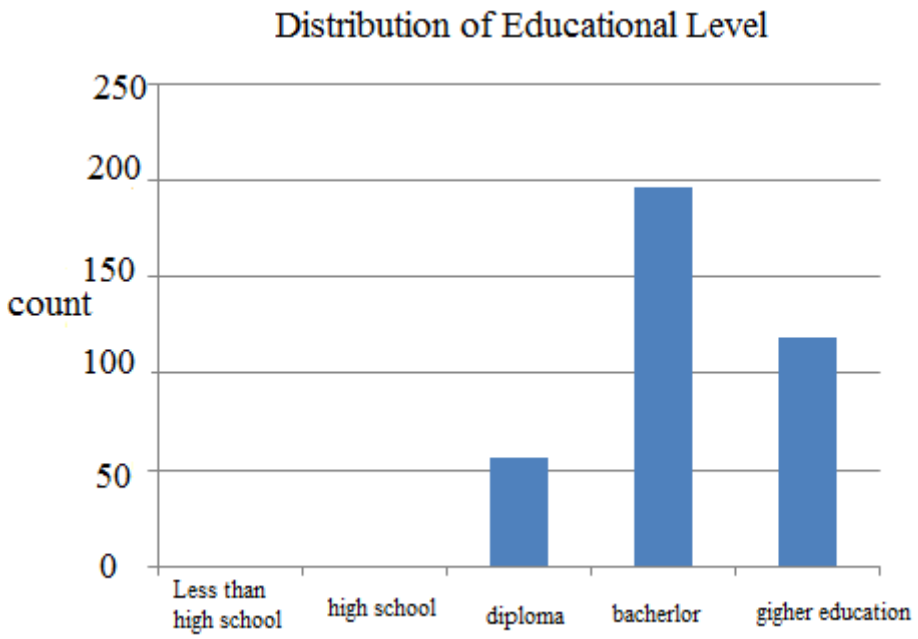


Figure 3: Respondents' distribution according to educational level

The number of single employees was 114 forming (30.65%), 258 with married employees (69.35%).

With regard to job title the respondents with normal Employee were the highest sector with 209 Employees forming (56.18%), followed by respondents with IT Employee with 61 Employees (16.39%);then the Heads of the Department were 38 forming (10.21%), whereas the smallest sector was for the Managers and Supervisors with only 12 for every one (3.22%). Finally the others were 40 Employees forming (10.75%).

Finally, the respondents with experience in information security less than ten years were the highest sector with 248 employees forming (66.66%), followed by respondents with 10-20 years' experience in information security with 93 employees (25%); whereas the smallest sector was for the

employees with experience more than 21 years were 31 employees forming (8.33%), This could be attributed to the young age of most employees.

4.2.2 Survey items' results

The second section of the questionnaire contained the actual measures used to measure the effect of each variable. For a smoother display of results, this section has been divided into five subsection, one for each construct; the mean and standard deviation for each construct as a whole were calculated and illustrated in tabular form, as well as the mean and standard deviation of each variable in the construct and displayed in a graphical form.

- **Individual Factors**

The variables of this construct were measured using the measures illustrated in Table 6 along with the mean and the standard deviation of each item

Table 6: Mean and standards deviation of Individual Factors items

	Variable' measure	Mean	St. Dev.
	Individual Factors		
	Neuroticism		
1.	I don't feel afraid nor stressed while working through using a computer.	3.9	1.08
2.	I don't feel that my value is lower than the value of my work colleagues	3.85	0.84
3.	I don't feel that I will have a nervous breakdown while working under a huge pressure	3.97	0.98
4.	I don't feel angry about the way I am treated	3.72	1.01
5.	I don't have a pessimistic view towards life	3.94	0.97
6.	I don't feel sometimes depressed and helpless.	3.66	1.04
	Extraversion		

7.	People perceive me as a cheerful, and active person who is full of energy	4.02	0.81
8.	I respond to jokes and smile fast	4.14	0.75
9.	I enjoy talking to people	4.08	0.74
10.	I love being friendly and nice with others	4.32	0.67
11.	I have a broad social relationship network	3.96	0.88
	Openness		
12.	I am keen to illustrate my opinion	3.38	1.04
13.	Using imagination and meditation participates in organizing time	3.16	1.09
14.	I love travelling and visiting new places	3.75	0.86
15.	I see beauty in the things that people perceive as being ordinary	3.22	1.05
16.	I enjoy reading books and periodicals	3.31	1.05
17.	I highly enjoy reading journals, and magazines, and surfing social media websites	3.2	1.04
	Agreeableness		
18.	I exert much effort in order to meet my goals	4.13	0.69
19.	I help my work colleagues much	3.94	0.68
20.	I don't like hurting others' feelings	4.01	0.81
21.	I carry out my work tasks accurately and efficiently	4.18	0.68
22.	I forgive the ones who did a disservice to me	4.14	0.67
	Conscientiousness		
23.	I seek organizing my stuff and ensuring that the area clean.	4.32	0.71
24.	I seek showing compliance with the institution's bylaw	4.33	0.63
25.	I keep working - without stopping - till I finish my work	4.3	0.62
26.	I seek finishing my works before the due time and without receiving help from anyone.	4.15	0.64
37.	People depend much on me. They trust me much	4.2	0.45
	Moral		
31.	I protect the institution's assets, including the institution's devices and apparatus	4.5	0.63
32.	When there is a problem at work, I exert effort to solve it instantly	4.33	0.63
33.	I am ready to handle the responsibility for my wrong acts	4.41	0.57
34.	I highly respect my work colleagues and I don't like talking about them	4.3	0.66
35.	I refrain from disclosing classified information to other institutions	4.55	0.64
36.	I search for methods and means that can improve my work performance	4.38	0.68
	The Average of the Construct	**3.99**	**0.79**

Individual Factors consisted of six variables: Extraversion, Agreeableness, Conscientiousness and Moral. Each of these variables was measured using at least 5 items. The averages of the mean and standard deviation of these variables are as illustrated in Figure 4. Most respondents ranked Extraversion, Agreeableness, Conscientiousness and Moral of the Individual Factors in a higher level of importance than Neuroticism and Openness which had the lowest mean among the six variables.

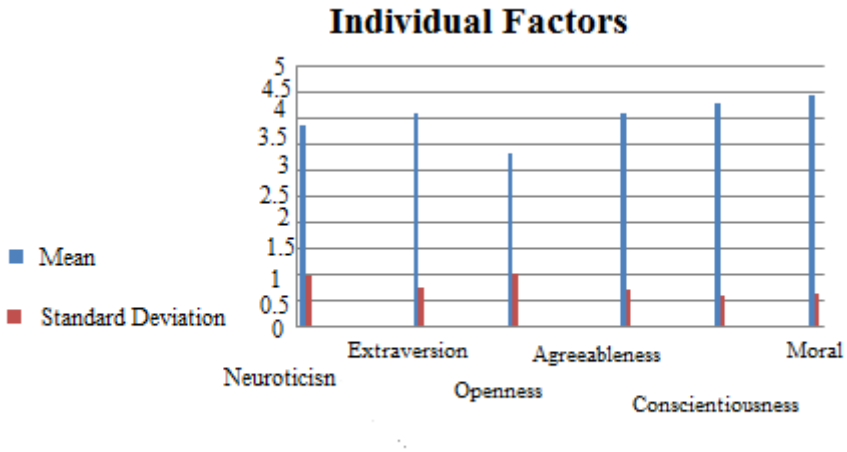


Figure 4: The mean and standard deviation of each variable in Individual Factors

➢ Employee satisfaction

Employee satisfaction is a standalone construct that has no sub variables. The mean of all questions was 3.52 and standard deviation of 0.95. The mean is appropriate, meaning that respondents agreed that these items should be available in Compliance with Information Security Policies. Six items were used to measure this construct; the mean and the standard deviation of each item are illustrated in Table 7.

Table 7: Mean and standards deviation of Employee satisfaction

	Variable' measure	Mean	St. Dev.
	Employee satisfaction		
1.	I am satisfied with my current basic salary when comparing it with the amount of tasks and responsibilities that I must handle	3.22	1.12
2.	My job security level in the institution I work at is high	3.62	1.04
3.	My direct supervisor deals in a fair manner with me	3.76	0.87
4.	The moral incentives that I receive from my direct supervisor increase my productivity	3.92	0.91
5.	I go in a bad mood in case I committed a fault that represents noncompliance with the institution's policies	3.52	0.71
6.	I highly believe that the institution I work at retains the outstanding employees	3.48	1.09
	The Average of the Construct	**3.58**	**0.95**

- **Organizational Factors**

The third construct is Organizational Factors. The measures that were used for this construct as well as the mean and standard deviation of each item are shown in Table 8:

Table 8: Mean and standard deviation Organizational Factors.

	Variable' measure	Mean	St. Dev.
	Organizational Factors		
	Support		
1.	If I faced a problem, I receive support from the institution's management	3.67	0.9
2.	If I faced a problem, I receive support from my work colleagues	3.97	0.71
3.	The institution's management seeks ensuring that the employees understand the goals.	3.78	0.82
4.	Periodical reports are delivered about the extent of meeting the goals	3.73	0.87
5.	I feel that my contribution to the institution are valuable and significant	4.06	0.75
6.	I receive adequate attention from the institution's management	3.47	1.03
	Training		
7.	I am provided with the needed training that enables me to meet my professional needs	3.35	1.05

8.	I receive the needed training about the information security policies	3.15	1.08
9.	The training I receive enables me to improve my professional skills	3.77	0.83
10.	The institution's management provides employees with training regularly	3.25	1.04
11.	I receive theoretical and practical training	3.3	1.05
12.	I receive training courses that suit my institutional position	3.2	1.03
	Culture		
13..	My institution provides much attention to the aspects related to the employee's personality. That is because the institution's management believes that all the employees are a big family	3.43	1.04
14.	The institution's management seeks establishing an innovative culture	3.38	1.04
15.	The institutional culture of my institution participates in building stable relationships between employees	3.55	1.02
16.	The institution's management of my institution encourages employees to excel at work	3.55	1.06
17.	The institutional culture of my institution participates in meeting the goals and raising productivity	3.55	1.02
18.	The institution's management of my institution seeks developing human resources	3.49	1.01
	The Average of the Construct	**3.53**	**0.96**

This construct was divided into three variables: support, training and Culture. The mean and standard deviation of these variables are illustrated in Figure 5. All of variables were measured using six measures.

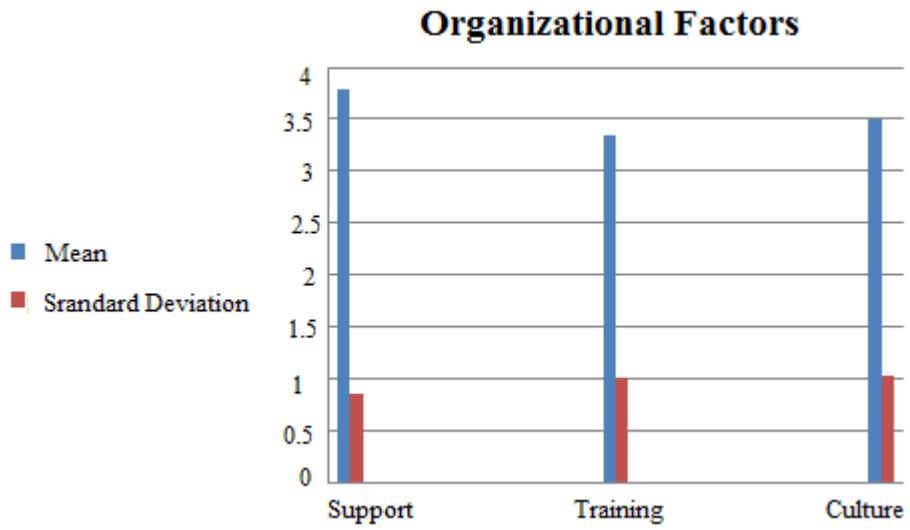


Figure 5: The mean and standard deviation of each variable in Organizational Factors

- **Technological Work Environment**

The forth construct Technological Work Environment is a standalone construct that has no sub variables. The mean of all questions was 3.77 and standard deviation of 0.94. Seven items were used to measure this construct; the mean and the standard deviation of each item are illustrated in Table 9.

Table 9: Mean and standard deviation of Technological Work Environment

	Variable' measure	Mean	St. Dev.
	Technological Work Environment		
1.	The institution has programs for protecting all its devices. These programs uploaded in a regular manner	3.89	0.88
2.	The institution's communication channels are characterized with transferring information smoothly	3.76	0.88
3.	The workplace is well-lit	4.1	0.74
4.	The workplace includes office supplies and great decorations	3.59	1.1
5.	There are modern and advanced devices at the workplace	3.84	0.89
6.	The availability of air condition devices in my office enables me to focus in work	3.62	1.17
7.	The workplace is characterized with being far away from the city center and noise	3.64	0.94
	The Average of the Construct	**3.77**	**0.94**

The last construct was the construct of the dependent variable, Compliance with the information security policies. The measures that were used for this construct as well as the mean and standard deviation of each item are shown in Table 10. The mean and standard deviation of the construct were 4.16 and 0.71 respectively.

Table 10: Mean and standard deviation of Compliance with the information security policies

	Variable' measure	Mean	St. Dev.
	Compliance with the information security policies.		
1.	I believe that practicing my profession requires acknowledging the institution's bylaws, regulations, and instructions.	4.17	0.66
2.	The policies and procedures related to information access are clear	4.02	0.75
3.	All the employees acknowledge the information security policy. There has been an agreement reached on the latter policy	3.89	0.85
4.	The password that I use consists from a mixture of words, numbers, and letters	4.33	0.72
5.	When going on a break or to the bathroom, I shut down my computer	4.15	0.69
6.	I don't download files from websites that are not well-known	4.13	0.61
7.	I instantly report any bug gets detected in the system	4.18	0.76
8.	I protect my personal information. I consider protecting such information as something important	4.43	0.69
9.	When using my institution's devices, I don't use a wireless network of any other institution	4.16	0.77
10.	I make backup copies for the important files	4.14	0.68
	The Average of the Construct	**4.16**	**0.71**

4.3 Structural Modeling Results

The significance of the path coefficients and the loadings were used to test the structural model (illustrating the strengths of relationships between independent and dependent variables), and the R^2 value (the variance amount explained by independent variables). A Smart PLS bootstrapping method was used to estimate the statistical significance of each path utilizing 300 samples to obtain t-values (Chin, 1998). It also needed to calculate the P-value. In the first running of the PLS algorithm, some unreliable item loading was yielded (<0.5). Figure 6 shows these results. The unreliable items, ones with loadings less than 0.5, were deleted and the final measurements and structural model are illustrated in Figure 6. In table

11, the final results of the PLS analysis on the structural model are presented, along with the t-values, path estimates and P-values. The study hypotheses are labelled on their corresponding paths in Figure 6 and support for them could be established by looking at the directionality (negative or positive) of the path coefficients and the meaning of the t-values. It is expected that the standardized path coefficients will be at least 0.2, and ideally, greater than 0.3 (Chin 1998). The P-value is defined as the error probability. Thus, if this relation works 95 **%** of the time, this means that the association has been accepted by this study. According to Greenland et al. (2016) an acceptable relationship between variables of the P-value is less than 0.05.

➢ P-values ranging from 0.05 to 0.01 = a significant relationship.

➢ P-values less than 0.01 = a strong significant relationship.

It was suggested by Chin (1998) that the values of R^2 that are above 0.67 are considered to be high, whilst values ranging from 0.33 to 0.67 are moderate, values between 0.19 to 0.33 are weak and any R^2 values less than 0.19 are unacceptable. A different minimum acceptable value of R-squared of 0.10 is suggested by Falk and Miller (1992).

The R^2 values for the dependent variables Information Security Compliance Policies is 0.481. This result reveal that the Information Security Compliance Policies about 48.1% of employee, R^2 is moderate.

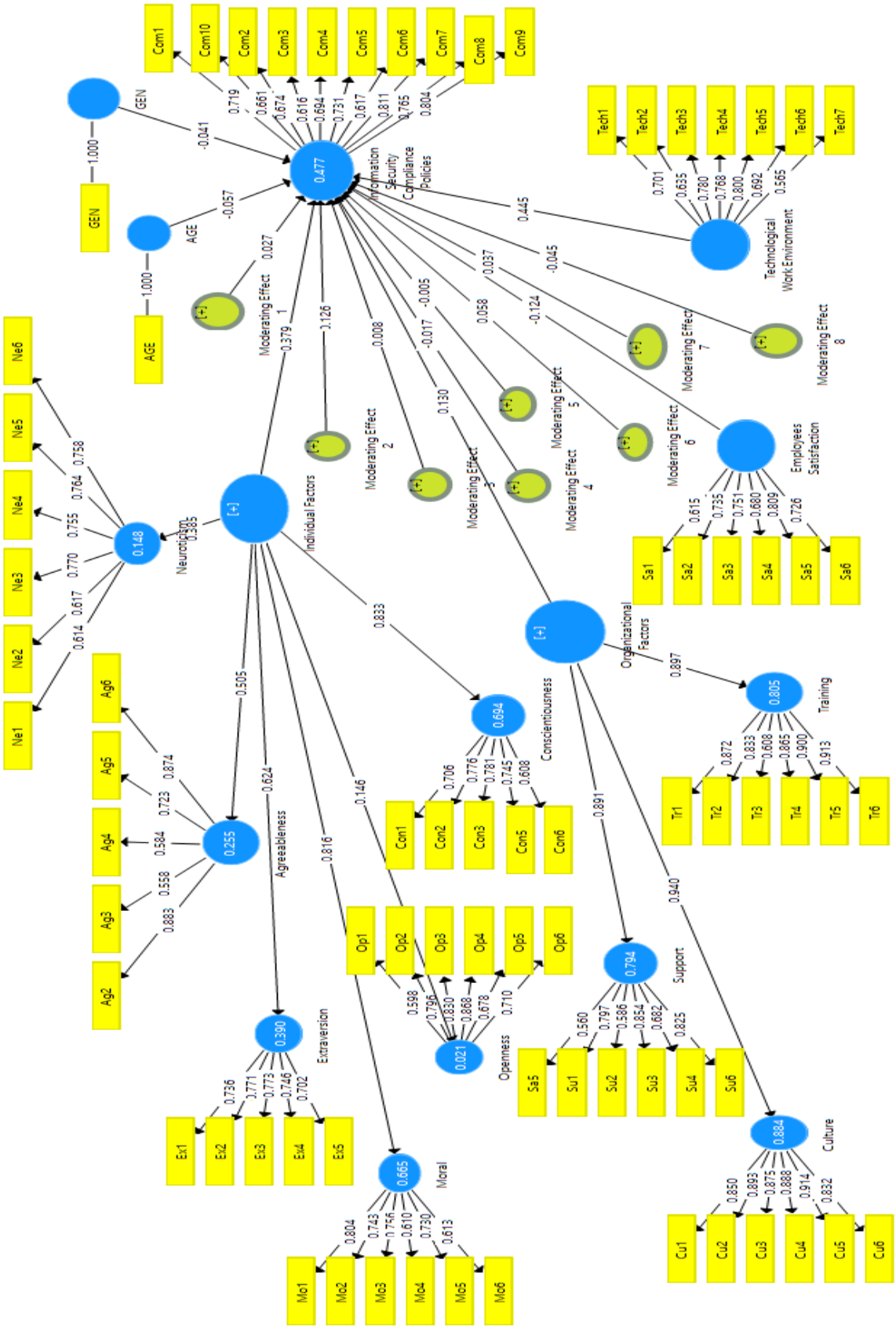


Figure 6: Measurement and Structural Model Results

Goodness-of-fit measures are not provided by Smart PLS software for the full path model as in LISREL and AMOS; it only provides R^2 values for the dependent variables. However, Tenenhaus et al. (2005) defined GoF as the fit global measure. It is the geometric mean of both average variance extracted (AVE) and R-squared of the endogenous variables. GoF's purpose is to account for the study model at both the levels of measurement and structural model, with a focus on the overarching performance of the model (Chin, 2010; Henseler & Sarstedt, 2013). The GoF formula is calculated as follows:

$$GoF = \sqrt{(\overline{R^2} \times \overline{AVE})}$$

Where AVE represent the average of all AVE values for the research variables while R^2 represents the average of all R^2 values in the full path model. The calculated global goodness of fit (GoF) is 0.49, which exceeds the recommended threshold of GoF>0.36 suggested by Wetzels et al. (2009). Thus, this study concludes that the research model provides an overall goodness of fit.

Table 11: Results of Structural Equation Model Analysis

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values	Supported/ Not Supported
Employees Satisfaction -> Information Security Compliance Policies	-0.124	-0.107	0.052	2.407	**0.016**	**Supported***
Individual Factors -> Information Security Compliance Policies	0.379	0.377	0.045	8.462	**0.000**	**Supported****
Moderating Effect 1 -> Information Security Compliance Policies	0.027	0.022	0.045	0.589	**0.556**	**Not Supported**
Moderating Effect 2 -> Information Security Compliance Policies	0.126	0.131	0.057	2.190	**0.029**	**Supported***
Moderating Effect 3 -> Information Security Compliance Policies	0.008	0.005	0.057	0.141	**0.888**	**Not Supported**
Moderating Effect 4 -> Information Security Compliance Policies	-0.017	-0.015	0.064	0.258	**0.797**	**Not Supported**
Moderating Effect 5 -> Information Security Compliance Policies	-0.005	-0.005	0.039	0.121	**0.904**	**Not Supported**
Moderating Effect 6 -> Information Security Compliance Policies	0.058	0.062	0.066	0.889	**0.375**	**Not Supported**
Moderating Effect 7 -> Information Security Compliance Policies	0.037	0.030	0.060	0.617	**0.537**	**Not Supported**

Moderating Effect 8 -> Information Security Compliance Policies	-0.045	-0.046	0.058	0.783	**0.434**	**Not Supported**
Organizational Factors -> Information Security Compliance Policies	0.130	0.118	0.065	2.012	**0.045**	**Supported***
Technological Work Environment -> Information Security Compliance Policies	0.445	0.451	0.050	8.893	**0.000**	**Supported****

Significant at P= < 0.01, p* <0.05**

The relative effect of a specific exogenous latent variable on endogenous latent variable(s) is indicated by changes in the R-squared (Chin, 1998). It is calculated as the increase of the latent variable in R-squared to which the path is connected, in relation to the latent variable's proportion of unexplained variance (Chin, 1998). The following formula can be used to convey the effect size (Cohen, 1988; Selya et al., 2012)

$$f^2 = \frac{R^2_{included} - R^2_{excluded}}{1 - R^2_{included}}$$

According to Cohen (1988) an Interpreting Effect Size (f2) assessed as follow:

- f2 above 0.35 are considered large effect size.
- f2 ranging from 0.15 to 0.35 are medium effect size .
- f2 between 0.02 to 0.15 considered small effect size.
- f2 values less than 0.02 are considering with NO effect size .

There are an effect size of dependent variables of Information Security Compliance Policies by variables Individual Factors are 0.245 and Technological Work Environment are 0.200, so it had medium effect size.

Using PLS for prediction purposes requires a measure of predictive capability. The suggested approach to test predictive relevance is called the Blindfolding procedure. According to Wold (1982), "The cross-validation test of Stone (1974) and Geisser (1975) fits soft modeling like hand in

glove". The procedure will remove data from the data set based on a pre-determined distance value called D. The D can be any number from 5-10 (Chin 2010). The only requirement is that the sample size n divided by D should be a round number.

According to Fornell and Cha (1994) a cv-red value of >0 shows that there is predictive relevance while a value of <0 indicates the model lacks predictive relevance.

Table 12: shows the Construct Cross validated Redundancy

Total of Q^2	Q^2 (=1-SSE/SSO)
Information Security Compliance Policies	0.215

As its shown in Table 12 , The Predictive Relevance was concerned about the total effect on the endogenous variable ,the values of Q^2 (=1-SSE/SSO) is greater than Zero, which support the claim that this study model has adequate ability to predict

4.4 Evaluating Moderating Effects

4.4.1 Age as a moderator

Testing moderating effects involves comparing a “main effect” model and a moderating effect model (Carte & Russell.2003) and (Chin et al., 2003), and meeting two conditions that moderation should be significant and should assist the intention "Increase or Decrease". The interaction terms were calculated by multiplying the moderator (age) by the predictor variables (Individual Factors and Information Security Compliance

Polices), (Organizational Factors and Information Security Compliance Polices), (Technological Work Environment and Information Security Compliance Polices) and (Employees Satisfaction and Information Security Compliance Polices) respectively. The moderating effects model included these interaction variables, while the main effects model did not. However, because the moderating effect of age on the influence of Information Security Compliance for Individual Factors. Technological Work Environment and Employees Satisfaction was found to be insignificant, so the test only was performed for the effect of the interaction of Organizational Factors with the age, the interaction of Organizational Factors with the Age is significant, the P-value and β are found to be 0.029 and 0.126 respectively. Figure 7 shows the interaction of Organizational Factors with age:

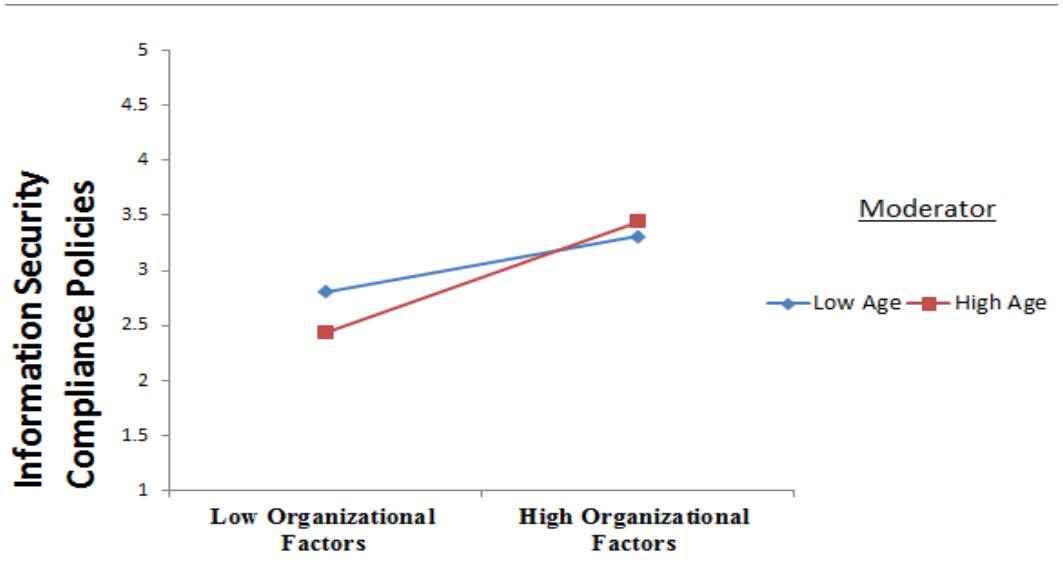


Figure 7: Age as moderator "Relationship between Organizational Factors and Information Security Compliance Policies.

Note: Low age: 18 - 38 years old, High age: Older than 38 years old, Low and higher organizational factors have been identified according to likert scale (Low: 1-2, and high: 4-5).

Age strengthens the positive relationship between organizational factors and information security compliance policies.

4.4.2 Gender as a moderator

The interaction terms were calculated by multiplying the moderator (gender) by the predictor variables (Individual Factors and Information Security Compliance Polices), (Organizational Factors and Information Security Compliance Polices), (Technological Work Environment and Information Security Compliance Polices) and (Employees Satisfaction and Information Security Compliance Polices) respectively. The moderating effect of gender on the influence of Information Security Compliance on Individual Factors, Organizational Factors, Technological Work Environment and Employees Satisfaction was insignificant, so this study proves that no differences between male and female.

4.4 Discussion of Results

The results in Table 11 and Figure 6 provide support for four main hypotheses (H1, H2, H3 and H4). Hypothesis 1 posited a significant influence relationship between Individual Factors and Information Security Compliance Policy. Consistent with H1, the result in Table 6 and Figure 6, indicates that there is a strongly significant (P-value = 0.000) positive (β=

0.379) relationship between Individual Factors and Information Security Compliance Policy. Hypothesis 2 posited a positive relationship between Technological Work Environment and Information Security Compliance Policy. Hypothesis 2, results indicated that Technological Work Environment is positively relationship with Information Security Compliance Policy (β = 0.445) and the relationship is strongly significant (P-value = 0.000). This is consistent with the prediction of H2 and is therefore supported. The standardized coefficient and significant levels of Employees Satisfaction (β = -0.124 ;(P-value = 0.016) is negative and significant. This is consistent with the prediction of H3 and it's supported. Thus, a higher level of Employees Satisfaction is associated with higher levels of Information Security Compliance Policy. The results in Table 11 and Figure 6 are in line with H4, leading that the higher the level of Organizational Factors, the higher the likelihood of Information Security Compliance Policy (β =0.130); (P-value = 0.045). Therefore, H4 is supported. Some researcher like D'Arcy and Greene (2014) found that organizational support had either a negative or insignificant relationship to security behaviors.

Hypotheses (H5a, H5b, H5c and H5d) posited that Age moderates the relation between (Individual Factors, Organizational Factors, Technological Work Environment and Employees Satisfaction) and Information Security Compliance Policies in such a way that the relationship is weaker for older workers compared to younger ones respectively. The result indicated that a strongly significant interaction of

Organizational Factors with Age, H5b (P-vale = 0.029) positive (β= 0.126), However, the results that has been analysis by Excel software shows that the age strength relationship between the Organizational Factors and Information Security Compliance Policies is positive. According to figure 7, the results shows that older workers are more committed to Information Security Compliance Policies compared to younger workers respectively. The results shows that the younger employees change their commitment slightly if the organizational factor varies from low to high level. While the older employers increase significantly their commitment to increase significantly if the level of the organizational factor varies from low to high. Therefore, as far as the age of the employer has increased, their commitment to information security policies would be more, providing that the level of the organizational factor increases in terms of training, support and culture of the organization. Therefore, H5b is not supported.

Finally, Hypotheses (H6a, H6b, H6c and H6d) posited that Gender moderates the relation between (Individual Factors, Organizational Factors, Technological Work Environment and Employees Satisfaction) and Information Security Compliance Policies. The result indicated that insignificant interaction of Individual Factors, Organizational Factors, Technological Work Environment and Employees Satisfaction with gender. Therefore, H6a, H6b, H6c and H6d are not supported.

Chapter Five

Conclusions and Recommendations

5.1 Overview

This chapter presents the summarized results of the research and derives conclusions. Besides that it aims to suggest some recommendations regarding enhancing Compliance with Information Security Policies for employees in Palestine.

5.2 Conclusions

The purpose of this research is to identify the Individuals Factors of employees, Organizational factors, Technological Work Environment and Employees Satisfaction from different generations and examining their effects on Information security compliance Policies. In order to achieve objectives, the current research followed the quantitative approach in which a questionnaire was used to gather the required data for analysis. The data was analyzed using Smart PLS v3.2.7 software for the Structural Equation Modeling (SEM) technique in order to carry out a statistical analysis of the measurement and structural models. In particular, six main hypotheses were postulated. Each of these hypotheses was divided into sub hypotheses that related the sub factors of the independent constructs with the sub factors of Compliance. The findings have answered the research questions and achieved its objectives. To test the proposed hypotheses, data were collected from large service organizations in the West Bank in Palestine.

The empirical result supported all main the first five posited research hypotheses in a significant way but there is no influence of the last hypotheses. Important to note about the study findings is the fact that Individuals Factors of employees, Organizational factors, Technological Work and Environment Employees Satisfaction have influence on Information security compliance Policies, Organizational factors with age influence on Information security compliance Policies but there is no influence with gender on Information security compliance policies. On the other hand, Chan et al. (2005), Herath and Rao (2009b) and Hu et al., (2012) found the organizational support to be positively associated with compliance, but D'Arcy and Greene (2014) and Ng et al (2009) found that organizational support had either a negative or insignificant relationship to security behaviors, while our results find that organizational support had positive and significant. The findings of this study are important for both organizations owners and researchers. For organizations owners it can help them identifying the factors that influence employees compliance in Palestine and focus on some issues like that increasing the support to the employees would positively impact their commitment to the information security policies, trained employees are more committed to information security policies than others, and their skills got improved, organizations that seek to spread the creativity and excellence amongst the employees, they are more committed to information security policies than others, the work environment is necessary for employees. Employees who have a good working environment are more committed to information security policies,

the greater the satisfaction of employees, the greater their commitment to information security policies, the organization should be concerned about all staff and not differ between young and senior staff. On the other hand, for researchers it forms a first step on the way of building a comprehensive model of factors affecting employees' compliance in Palestine. They can benefit from the current study' findings and build on it to include other factors that are not included.

5.3 Recommendations

The current study analyzed the factors affecting on Compliance with Information Security Policies in Palestine.

The researcher came out with some recommendations for enhancing Compliance with Information Security Policies in Palestine. These recommendations are for organizations owners. The organizations owners should consider several actions and functions necessary for the success of Compliance with Information Security Policies in Palestine these include:

1- Increasing of organizational support for employees

The results show that increasing the support to the employees would positively impact their commitment to the information security policies. The organization should be concerned about the employees and provide help at some certain times, so the employee would be a part of the organization, which by this would lead to significant contribution to the organization development.

2- Conduct periodic training in information security

The results show that trained employees are more committed to information security policies than others, and their skills got improved likewise. We recommend for the organizations to conduct periodic training courses for employees to develop and improve their skills in compliance with information security policies.

3- The culture of the organization

The current study shows that organizations that seek to spread the creativity and excellence amongst the employees. They are more committed to information security policies than others, so the institution should not neglect this aspect and concern about spreading the culture of creativity and excellence among employees.

4- Work Environment

The results illustrate that the work environment is necessary for employees. Employees who have a good working environment are more committed to information security policies, so the organization should provide a suitable and good environment for employees, such as providing good lighting and quiet work atmosphere, offer wonderful and modern computers equipped with the best protection programs, and offering the employees smooth and clear channels for communication amongst themselves.

5- Increase employees satisfaction

The organization should be concerned about its employees satisfaction, the greater the satisfaction of employees, the greater their commitment to information security policies.

Therefore, the organization must be concerned about the employee and provide support to them, such as financially, managerial or any kind of support. In addition, offering a good salary according to their positions and studies. The employees would feel financially secured and encourage them to excel in work and also receive rewards for their distinction.

6- The age of Employees

The organization should be concerned about all staff and not differ between young and senior staff.

The results indicated that older workers are more committed to Information Security Compliance Policies compared to younger workers due to the long experience over years. Therefore, institutions and organizations should transfer this long experience to the new generations.

5.4 Limitations and Future Research

Although this study makes significant contributions to both academia and practice, it was limited in some ways, and therefore some future research avenues are suggested. First, the data were gathered from the West Bank of Palestine, the results would be more informative if the sample data

gathered from the Gaza strip. Therefore, future studies may be conducted by using data from Gaza strip, perhaps too, future studies should not be limited to Palestine, but rather consider extending this research to other Arab countries such as Jordan for results comparison. Future studies can also extend the current study by studying the relationships in the current conceptual model by long term of age.

References

- Abadu, A. (2013). **The relationship of the five major factors of personal satisfaction in a place Work,** Unpublished MA, Faculty of Humanities and Social Sciences, Department of Social Sciences، University of Qasdi Rabah, Algeria, 45.

- Abdalgani, A. (2001). **Industrial Psychology Foundations and Applications,** First Edition, Modern University Office, Alexandria, 374.

- AbdelKhaliq, A. (1998). **The basic dimensions of personality**, Dar al-Maarefa University for Printing and Publishing, Alexandria.

- Abdullah, M.A. (2007). **Industrial Psychology between Theory and Practice,** First Edition, Dar Al - Maarefah Al - Jamaiya, Alexandria.

- Abu-Musa, A. (2010). **Information Security Governance in Saudi Organizations: An Empirical Study**. Information Management &Computer Security, 18*(4),* 226 - 276.

- Aladili, N. (1981**). Job Satisfaction a field studies for directions and positions of employees of government agencies in Riyadh**, Saudi Arabia. Institute of Public Administration. Master's thesis in Administrative Psychology from the State University of California Humboldt, 14-16.

- Alaghbari, A. (2002). ***Job Satisfaction in a Sample of Directors of General Education Schools in the Eastern Region*** *(Field Study)* **Journal of Gulf and Arabian Peninsula Studies** 109, 169-197.

- Alahmed, H.A. (2008). **The Effect of Organizational Culture on the Development of Creative Behavior of Workers**. Applied Research on Spinning and Textile Institutions in Aleppo, Master Thesis (unpublished), Aleppo University, Syria.

- Alamro, S.A.(1996).**The Work Environment and its Relationship to the Injury of Civil Defense Man**, Unpublished Master Thesis, Riyadh, Naif Arab Academy for Security Sciences, 24.

- Alansari, B. (1997). ***The Effectiveness of the List of Five Major Factors of Personality in Society Kuwaiti***: **Journal of Psychological Studies, Egyptian Psychologists Association,** *1*(1), 277-310.

- Alanzi, F. (2007). **Obsessive-Compulsive Disorder and its Relation to The Five M Factors of Personality**, unpublished master thesis, Department of Social Sciences, Naif Arab University for Security Sciences, Riyadh, 1982-83.

- Alasawi, A., (1997). **Psychology of Labor and Workers**, First Edition, University Salary House, Beirut Lebanon.

- Albrechtsen, E. (2007). **A Qualitative Study of Users ' Vie On Information Security:** Computers &Security, 26(4), 276 -289.

- Albrechtsen, E., & Hovden, J. (2010**). Improving information security a wareness and behaviour through dialogue, participation and collective reflection: An intervention study.** Computers & Security, 29(4), 432–445.

- Alaswai, A. (1997). **Psychology of Labor and Workers**, First Edition, University Salary House, Beirut Lebanon.

- Ali, L. (2010). **The Relationship of Work Accidents to the Physical Conditions in the Professional Environment**, International Forum on Suffering at Work, University of Staif, Algeria, 45.

- Alkbesi, & Amer (1998). **Organizational Design**, First Edition, Dar Al Sharq Printing & Publishing, Doha. 87.

- Alkhafaki, N.A. (2009). **Culture of the Organization**, Dar Al-Yazuri Scientific Publishing and Distribution, Amman, Jordan, 21.

- Al-mayahi, I. H., & Sa'ad, P. M. (2014). ***Information Security Policy Development.*** **Journal of Advanced Management Science**, *2*(2).

- Almawafi, F.H., & Radi, F. M. (2006). ***The Psychometric Characteristics of the Five Questionnaire,*** **the Egyptian Journal of Psychological Studies:** The Egyptian Society for Psychological Studies, 16(53), 1-25.

- AlMosawi, S. (2004) **Human Resources Management and the effects of globalization on them**. Dar Majdlawi For publication, Amman, 1, 189**.**

- Alnamir, S. (1993). ***Job Satisfaction of the Saudian Employee in the Public and Private Sectors*****: King Saud University Journal**, Administrative Sciences, Master Thesis, 75.

- Al-Qariuti, M. Q. (2000a). **Organizational Behavior: A Study of Individual and Collective Human Behavior in Different Organizations**, Amman, Dar Al-Shorouk, 151.

- Al-Qariuti, M. Q. (2000b).**The Theory of The Organization and Organizing:** Dar Wael for printing and Publishing, Jordan, 228.

- Alsalem, H.A. (2006).**Optimism and Pessimism and Their Relation to The Five Factors of Personality in a Sample of Students of King Saud University**, unpublished master thesis, Department of Psychology, College of Education, King Saud University, Saudi Arabia, 80-85.

- Alsarayra, A. A. (2003). **The relationship between Organizational Culture and Management Innovation of Potash and Phosphate Companies Jordan Public Contribution:** Survey Study, Muta Research and Studies.

- Alshanti, M.A.I. (2006). **The Impact of the Organizational Climate on the Performance of Human Resources**, Master 's Thesis in Business Administration, Islamic University of Gaza, 34.

- Alshawani, S. (2003). **Human Resources and Human Relations Department.** Youth Foundation University, Alexandria.

- Alshekh, (2015). **Information System Security and Control.** Master Thesis, Demashq University, Syria.

- Altaani H. A. (2007), **Contemporary Management Training.** Dar Al-Masirah for Publishing, Amman, 1, 22.

- Ashenden, D. (2008). "**Information Security management: A human challenge?"** Information Security Technical Report, *13*(4), 195 – 201.

- Baron, R.M. & Kenny, D.A. (1986). ***"The moderator-mediator variable distinction in social psychology research: Conceptual, strategic, and statistical considerations",*** **Journal of Personality and Social Psychology,** *51*, 1173-1182.

- Beautement, A., & Sasse, A. (2009). **The Economics of User Effort in Information Security**. Computer Fraud & Security, *10*, 8 – 12.

- Bruk, C.S., Allen, D.T. (2003). ***The Relationship between Big Five Personality Traits, Negative Affectivity, Type a Behavior, and Work family Conflict.*** **Journal of Vocational Behavior**, 63, 457-472.

- Bulgurcu, B. Cavusoglu, H. & Benbasat, I. (2010). ***Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness***. MIS Quarterly 34(3), 523–548.

- Carte, T.A., and Russell, C.J. (2003). **In pursuit of moderation: Nine common errors and their solutions**. MIS Quarterly, 27(3), 479–501.

- Chan M., Woon I and Kankanhalli A. (2005). ***Perceptions of information security in the workplace: Linking information security climate to compliant behavior***. Journal of Information Privacy and Security 1(3), 18–41.

- Chang, S. E., and Ho, C. B. (2006). **Organizational factors to the effectiveness of implementing information security management**. Industrial Management &Data Systems, *106*(3), 345–361.

- Chin, W.W. (1998). **Issues and opinion on structural equation modelling**, MIS Quarterly, *22* (1), 7–16.

- Chin, W. W. (2010). How to write up and report PLS analyses. In Vinzi V. Esposito, W. W. Chin, J. Henseler, & H. Wang (Eds**.), Handbook of partial least squares: Concepts, methods and applications in marketing and related field**s (Springer Handbooks of Computational Statistics Series, II, 655–690). Berlin: Springer.

- Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). **A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study**. Information Systems Research, *14*, 189–217.

- Chin, W.W, & Newsted, P.R. (1999). **Structural Equation Modeling analysis with Small Samples Using Partial Least Squares**. In Rick Hoyle (Ed.), Statistical Strategies for Small Sample Research, *Sage Publications*, 307-341. Thousand Oaks, CA: Sage.

- Chin, W.W., Marcolin, B.L., & Newsted, P.R. (2003). **A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic mail emotion/adoption study**. Information Systems Research, *14*, 2, 189–217.

- Cohen, J. (1988). **Statistical power analysis for the behavioral sciences.** Mahwah, NJ: Lawrence Erlbaum.

- Gosling, S., Rentfrow, P., & Jr, W. (2003). ***A Very Brief Measure of the Big Five Personality Domains***. **Journal of Research in Personality**, *37*, 504-528.

- Costa, P. T., & McCrae, R. R. (1995). ***Primary traits of Eysenck's P.E.Nsystem: Three and five factor solution.*** **Journal of Personality and Social Psychology,** *69*, 308-317.

- Colquitt, J. A., Le Pine, J. A. & Noe, R. A. (2000). ***Toward an integrative theory of training motivation: A meta-analytic path analysis of 20 years of research*****, Journal of Applied Psychology**, *85*, 678-707.

- Colwill, C. (2009). **Human factors in information security: The insider threat-Who can you trust these days?** Information Security Technical Report, *14*(4), 186 – 196.

- Cram, W. A., Proudfoot, J. G. & D'Arcy J. (2017). ***Organizational Information Security Policies: A Review and Research Framework***. **European Journal of Information Systems**, *26*(6), 605-641.

- Conway, E. (2004). "***Relating career stage to attitudes towards HR practices and commitment: Evidence of interaction effects***?" **European Journal of Work and Organizational Psychology**, 13, 417-446.

- Da Raad, B. (2000). **The Big Five Personality Factor: The Psycholexical Approach to Personality**. Toronto: Hogrefe and Huber Publishers. 91- 96.

- Daft, R. L. (2004). **Organization Theory and Design.** 8th Edition, South Western a division of Thomson Learning.

- D'arcy, J. & Greene, G. (2014). **Security culture and the employment relationship as drivers of employees' security compliance**. Information Management and Computer Security, *22*(5), 474–489.

- D'arcy, J. Herath, T. & Shoss, M.K. (2014). ***Understanding employee responses to stressful information security requirements: A coping perspective.*** **Journal of Management Information Systems** *31*(2), 285–318.

- Daniel, W. W., & Cross, C. L. (2013). **Biostatistics: A Foundation for Analysis in the Health Sciences.** 10th edition. Wiley

- De Lange, A.H., de Taris, T.W., Jansen, P.G.W., Smulders, P., Houtman, I.L.D., & Kompier, M.A.J. (2006). **"Age as a factor in the relation between work and mental health: Results from the longitudinal TAS study",** in Houdmont J. and McIntyre S. (Eds.), Occupational health psychology: European perspectives on research, education and practice, *Maia: ISMAI Publication*, 1, 21–45.

- Dey, M. (2007). **Information Security Management – A Practical Approach**. Proceedings of the IEEE AFRICON, pp. 1 – 6. doi:10.1109/AFRCON.2007.4401528.

- Digman, J. M. (1990). ***Personality Structure: Emergence of the 5Factor Model.*** **Journal: Annual Review of Psychology**, *41*(1), 436

- Dinev, T. Goo, J. Hu, Q. & Nam, K, (2009). ***User behaviour towards protective information technologies: The role of national cultural differences***. **Information Systems Journal** *19*(4), 391–412.

- Dynes, S., Brechbühl, H., & Johnson, M. E. (2005). **"Information Security in the Extended Enterprise: Some Initial Results from a Field Study of an Industrial Firm"** Proc. 4h Workshop on the Economics of Information Security.

- Ebner, N. C., Freund, A. M. & Baltes, P. B. (2006). **"Developmental changes in personal goal orientations from young to late adulthood: from striving for gains to maintenance and prevention of losses",** Psychology and Aging, 21, 664–678.

- Edgar S. (1986). **Organizational Culture and Leadership,** 5th Ed. (The Jossey-Bass Business & Management Series.

- Eisenberger, R., Fasolo, P. & LaMastro, V.D. (1990). ***"Perceived Organizational Support and Employee Diligence, Commitment and Innovation",*** **Journal of Applied Psychology**, *75*,1,51.

- Eisenberger, R. Cummings, J. Armeli, S. & Lynch, P. (1997***)."Perceived Organizational Support, Discretionary Treatment, and Job Satisfaction",*** **Journal of Applied Psychology**, *82*(5), 812-820.

- Ewen, R. B. (1998). **An Introduction to Theories of Personality**. Mahwah: N.J: Lawrence Erlbaum Associates, 140.

- Faleh, F.A & AbdelMajeed, E.M. (2009). **Organizational Behavior in the Management of Educational Institutions,** *II,* Jordan, Dar Al - Massira.

- Falk, R. F., & Miller, N. B. (1992). **A primer for soft modeling**. Akron, OH: University of Akron Press.

- Farr, J.L., Tesluk, P.E., & Klein, S.R. (1998). **Organizational structure of the workplace and the older worker**, in Schaie K. W. and Schooler C. (Eds.), Impact of work on older adults. Societal impact on aging series, *New York: Springer, 19,* 143–206.

- Feng, N., Wang, H.J. & Li, M. (2014). **A Security Risk Analysis Model for Information Systems: Causal Relationships of Risk Factors and Vulnerability Propagation Analysis**. Information Sciences, *256*, pp. 57 – 73.

- Fincham, R. & Rhodes, P.S. (1999). **Principles of organizational behavior**. (3rd ed.). New York: Oxford. University press.

- Fornell, C. & Cha, J. (1994). **Partial Least Squares**. Advanced Methods of Marketing Research, 407, 52-78.

- Fornell, C., & Larcker, D.F. (1981). ***Evaluating structural equation models with unobservable variables and measurement error***. **Journal of Marketing Research**, *27,* 39–50.

- Foth, M. (2016). ***Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence.*** **European Journal of Information Systems** *25*(2), 91–109.

- Freund, A.M. (2006). A**ge-differential motivational consequences of optimization versus compensation focus in younger and older adults**, Psychology and Aging, 21, 240-252.

- Geisser, S. (1974). **A predictive approach to the random effects model**. *Biometrika*, *61*, 101–107.

- George, J.M. (1999). **"Organizational Behavior"**, Addison-Welsey Publishing Company, N.Y, 320.

- Gillies, A. (2011). ***Improving The Quality of Information Security Management Systems With ISO 27000***.**TheTotal Quality Management Journal,** 23(4), 367 – 376.

- Glaspie, H.W., & Karwowski, W. (2018). **Human Factors in Information Security Culture: A Literature Review**. In: Nicholson D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2017. Advances in Intelligent Systems and Computing, 593. Springer, Cham.

- Goo, J., Yim, M.S., & Kim, D.J. (2014). **A path to successful management of employee security compliance: An empirical study of information security climate.** IEEE Transactions on Professional Communication 57(4), 286–308.

- Gonzalez, J.J. & Sawicka, A. (2002). **A Framework for Human Factors in Information Security.** In: Proceedings of the 2002 WSEAS International Conference on Information Security (ICIS'02), Rio De Janeiro.

- Greenberg, J. (2002). **Who stole the money, and when? Individual and situational determinants of employee theft**. Organizational Behavior and Human Decision Processes 89(1), 985–1003.

- Greenland, S., Senn, S. J., Rothman, K. J., Carlin, J. B., Poole, C., Goodman, S. N., & Altman, D. G. (2016). ***Statistical tests, P values, confidence intervals, and power: a guide to misinterpretations***. **European journal of epidemiology,** *31*(4), 337-50.

- Guo, K. H., Yuan, Y., Archer, N.P. & Connelly, C. E. (2011) ***Understanding no malicious security violations in the workplace: A composite behavior model***. **Journal of Management Information Systems** *28*(2), 203–236.

- Hair, F. J., Hult, G.T. M., Ringle, C.M., & Sarstedt, M. (2017). **A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM),** Second Edition, SAGE Publications, Inc. P 69.

- Hanan, A.M. (2006). **Health and Safety Note and its Impact on Productivity Efficiency in the Industrial Corporation**, Human Resources Management, Montessori University, Constantine, p. 49-51.

- Hareem, H. & Alsaaed, R. (2006). ***"Organizational Culture and its Impact on Building Organizational Knowledge: An Empirical Study in Jordanian Banking Divides:*** **Jordan Journal of Business Administration**, *2*(2), 230.

- Hareem, H. (2010**). Department of Organizations Holistic Perspective,** Dar Al-Hamed, Second Edition, Amman, Jordan, 257.

- Harkins, M. (2012). **Managing Risk and Information Security:** Protect to Enable: A press.

- Halsall A. K. (2017). **Generation X and Generation Y: What's the Difference?** [Online] Available at: https://www.huffingtonpost.com/quora/generation-x-and generati_b_6672780.html [Accessed 10 January 2019].

- Haredi, A.M. & Shawqi, F.L. (2002). ***Sources of Happiness Conscious in Light of the Five Major Factors of Personality, Religiousness and Some Other Variables,*** **Journal of Psychology**, *Cairo,* 46-78.

- Henseler, J., & Sarstedt, M. (2013). **Goodness-of-fit indices for partial least squares path modeling**. Computational Statistics, 28, 565–580.

- Herath, T., Herath, H., & Bremser, W. G. (2010). **Balanced scorecard implementation of security strategies: a framework for IT security performance management.** Information Systems Management, *27*(1), 72-81.

- Herath, T., & Rao, H. R. (2009a). **Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness**. Decision Support Systems, 47(2), 32.

- Herath, T., & Rao, H. R (2009b). ***Protection motivation and deterrence: A framework for security policy compliance in organizations***. **European Journal of Information Systems** *18*(2), 106–125.

- Hogan, R.T. (1983). **Socio-analytic theory of personality. In I982 Nebraska Symposium on Motivation: Personality-Current Theory and Research.** Univ. of Nebraska Press, Lincoln, Neb.

- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). **Managing employee compliance with information security policies: The critical role of top management and organizational culture**. Decision Sciences, 43(4), 615–659.

- Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). **Does deterrence work in reducing information security policy abuse by employees?** Communications of the ACM 54(6), 54–60.

- Hulland, J. (1999). ***Use of Partial Least Squares (PLS)' in Strategic Management Research: A Review of Four Recent Studies***. **Strategic Management Journal,** *20* (2): 195-204.

- Howard, P.J., Howard, J.M. (1995). **The Big Five Quick start: An Introduction to the Five-Factor Model of Personality for Human Resource Professionals,** Center for Applied Cognitive Studies (CentACS), Charlotte, North Carolina.

- Ifinedo, P. (2012). **Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory**. Computers & Security, *31*(1), 83-95.

- Ifinedo, P. (2014). **Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition**. Information and Management *51*(1), 69–79.

- Chaula, J. A., Yngström, L. & Kowalski, S. (2006)**. Technology as a Tool for Fighting Poverty: How Culture in the Developing World Affect the Security of Information Systems**, Proceedings of the 4th IEEE International Workshop on Technology for Education in Developing Countries (TEDC'06),4.

- Johnston, A.C., Warkentin, M., Mcbride, M., & Carter, L. (2016). ***Dispositional and situational factors: Influences on information security policy violations***. **European Journal of Information Systems** *25*(3), 231–251.

- Joppe, M. (2000). **The Research Process**. Retrieved from https://www.ukessays.com/essays/psychology/the-reliability-and-validity-psychology-essay.php?vref=1 . [Accessed 5 February 2019].

- Kanfer, R. & Ackerman, P. (2004). **Aging, Adult Development, and Work Motivation,** the Academy of Management Review, *29*, 440-458.

- Kayworth, T. and Whitten, D. (2010). **Effective Information Security Requires Balance Of Social And Technology Factors**, MIS Quarterly Executive, 9(3), 163 – 175.

- Kim, S.S., & Kim, Y.J. (2017). ***The Effect of Compliance Knowledge and Compliance Support Systems on Information Security Compliance Behavior***, **Journal of Knowledge Management**, *21*(4), 986 – 1010.

- Kooij, D.T., Jansen, P.W.G., Dikkers, J.S.E. & De Lange, A.H. (2010). ***The influence of Age on the associations between HR practices and both affective commitment and job satisfaction: A meta-analysis***, **Journal of Organizational Behavior,** 31, 1111-1136.

- Kwon, J., Ulmer, J. R., & Wang, T. (2012). ***The association between top management involvement and compensation and information security breaches.*** **Journal of Information Systems**, *27*(1), 219–236.

- Landy, F.J. & Trumbo, D.A (1980). **Psychology of Work Behavior,** revised edn. Homewood, IL: Dorsey Press.

- Line, M. B., Tondel, I. A., & Jaatun, M. G. (2011). **Cyber security challenges in Smart Grids. Paper presented at the Innovative Smart Grid Technologies (ISGT Europe),** 2nd IEE PES International Conference and Exhibition on.

- Lissitsa, S. & Kol, O. (2016). ***Generation X vs. Generation Y – A decade of online shopping***, **Journal of Retailing and Consumer Services,** 31,3.

- Linden, D., Nijenhuis, J., & Barkker, A. (2010). ***The general Factor of Personality: A meta-analysis of Big Five Inter-correlations and a criterion-related validity study***. **Journal of Research in Personality**, *44*, 315-327.

- Leisink, P.L.M. & Knies, E. (2011). ***Line managers' support for older workers***, **The International Journal of Human Resource Management**, *22*, 1902–1917.

- Loster, P. C. (2005). **Managing e-business risk to mitigate loss**. Financial Executive, 21(5), 43–45.

- Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). ***Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organizational information security policies: An empirical study of the influence of counterfactual reasoning and organizational trust***. **Information Systems Journal** *25*(3), 193–230.

- Maher, A. (2010). **Wages and Compensation Systems**, First Edition, University Publishing House, Alexandria.

- Mashaali, B. (2011). **Role of Professional Safety Programs in Improving the Performance of Workers in Small and Medium Enterprises in Algeria,** MA in Economics, Farahat Abbas Bastif University, Algeria, 79.

- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). **Individual Differences and Information Security Awareness.** Computers in Human Behavior, *69*, 151 – 156.

- Mohsen (2014). **Information Security Management in the Palestinian** Banks Year, Master Thesis, AN-Najah National University, Palestine.

- Moquin, R., & Wakefield, R. L. (2016). ***The roles of awareness, sanctions, and ethics in software compliance.*** **The Journal of Computer Information Systems** *56*(3), 261–270.

- Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. &Vance, A. (2009). ***What levels of moral reasoning and values explain adherence to information security rules? An empirical study***. **European Journal of Information Systems** *18*(2), 126–139.

- Ng, B.Y., Kankanhalli, A. & Xu, Y. (2009). **Studying users' computer security behavior: A health belief perspective.** Decision Support Systems 46(4), 815–825.

- Oates, B.J. (2006). **Researching Information Systems and Computing.** Middles borough UK: Sage Publications Ltd.

- Oguk, C. O., Karie, N. & Rabah K. (2017). ***Information Security Practices In Universities In Kenya.*** **Mara Research Journal of Computer Science & Security,** *2*(1), 61 – 73.

- Owadah, K.M. (1996). **Industrial Psychology**, Beirut, Dar al-Kuttab al-Alami.

- Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). **Human Factors and Information Security: Individual, Culture and Security Environment**. Report published by Defense Science and Technology Organization, DSTO-TR-2484, 1 – 45.

- Peretti, J.M. (2005*).* **Dictionnaire des Ressources Humaines**, 4e, Vuibert, Paris, 121.

- Posey C, Roberts Tl &Lowry P. B. (2015). ***The impact of organizational commitment on insiders' motivation to protect organizational information assets.*** **Journal of Management Information Systems** *32*(4), 179–214.

- Puhakainen, P., & Siponen, M. (2010). **Improving employees' compliance through information systems security training: An action research study.** MIS Quarterly 34(4), 757–778.

- Ringle, C. M., Wende, S., & Will, A. (2005). **Smart PLS 2 [Computer software].** Retrieved from http://www.smartpls.com. [Accessed 5 February 2019].

- Reisenwitz, T. H., Iyer, R. (2009). ***Differences in Generation X and Generation Y: Implications for the Organization and Marketers,*** **the Marketing Management Journal,** *19* (2), 91 – 103.

- Saeed, S.M. (1987). ***The Organizational Climate***, **the Arab Journal of Management, Amman**, 49.

- Salah, E.M.A. (2004**). Human Resources Department**, "Contemporary Application Approach", University Press, Alexandria.

- Saucier, G. (2002). ***Orthogonal Marker for Orthogonal Factor: The Case of the Big Five***. **Journal of Research in Personality**, *36*, 1-31.

- Saunders, M. N. (2011). **Research methods for business students**, 5/e. Pearson Education India.

- Saunders, M., Lewis, P., & Thornhill, A. (2009). **Understanding research philosophies and approaches**. Research methods for business students, 4, 106-135.

- Sekiou, L., (1999). **Human Resources in the Globalization Context of Markets.**4é, Boeck Université, Montréal, 299.

- Sekiou, L., (2004**). Human Resource Management** .Édition de Boeck Université, Montréal, 377.

- Selya, S.A., Rose, S.J., Dierker, C.L., Hedeker, D. & Mermelstein, J.R. (2012). **A Practical Guide to Calculating Cohen's F 2, A Measure of Local Effect Size, From Proc Mixed**, Frontiers in Psychology, 2.

- Settersen, R.A. Jr. & Mayer, K.U. (1997). **The measurement of age, age structuring, and the life course,** Annual Review of Sociology, 23, 233-61.

- Shawish, M. (2004). **Human Resources Management**, "Personnel Management", (i), 3 Oman: Dar Al Shorouk, 111.

- Shore, L. & Tetrick, L. (1991). ***A Construct Validity Study of the Survey of Perceived Organizational Support***, **Journal of Applied Psychology,** 76(5), 637-643.

- Shropshire, J., Warkentin, M. & Sharma, S. (2015). **Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior**, Computers & Security, *49*, 177 - 191.

- Singh B.S.P. & Malhotra, M. (2015). "***The Mediating Role of Trust in the relationship between Perceived Organizational Support and Silence",*** **International Journal of Scientific and Research Publications**, *5*(9) 2.

- Siponen, M. & Iivari, J. (2006). ***Six design theories for IS security policies and guidelines.*** **Journal of the Association for Information Systems** *7*(7), 445–472.

- Siponen, M. & Willison, R. (2009). **Information Security Management Standards: Problems and Solutions,** Information and Management, 46(5), 267 – 270.

- Siponen, M., Pahnila, S., & Mahmood, A. M. (2006). **A New Model for Understanding Users' IS Security Compliance,** The Tenth Pacific Asia Conference on Information Systems (PACIS), 644 – 657.

- Siponen, M. T. (2001). **An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications, In: Information Security Management: Global Challenges in the New Millennium, Dhillon, G. (ed.)**. Idea Group Publishing, Hershey.

- Siponen, M. T. & Oinas-Kukkonen, H. (2007). **"A Review of Information Security Issues and Respective Research Contributions**," ACM SIGMIS Database: the Database for Advances in Information Systems, 38(1), 60 – 80.

- Siponen M, Pahnila, S. & Mahmood, M.A. (2010). **Compliance with information security policies: An empirical investigation**. Computer 43(2), 64–71.

- Solms, R.V., Solms, S.H.V., & Caelli, W.J. (1993). **A Model for Information Security Management**, Information Management and Computer Security, 1(3), 12 – 17.

- Soomro, Z. A., Shah, M. H. & Ahmed, J. (2016). ***Information Security Management Needs More Holistic Approach: A Literature Review,*** **International Journal Of Information Management**, *36*(2), 215 – 225.

- Sterns, H., Subich, L.M. & Feldman, D. C. (2002). **Work careers: a developmental perspective,** San Francisco, Jossey-Bass.

- Stewart, J. M., Chapple, M., & Gibson, D. (2012). **CISSP: Certified Information Systems Security Professional Study Guide**: John Wiley & Sons.

- Stone, M. (1974). ***Cross-validatory choice and assessment of statistical predictions.*** **Journal of the Royal Statistical Society**, *36*, 111–147.

- Sui, Y., Zou, X., Du, Y., & Li, F. (2012). **Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method.** IEEE Transactions on Computers, *63*(4), 902-916.

- Taha, F.A. (1985). **Industrial and Organizational Psychology**, 5th ed., and Distribution, Alexandria, Dar al-Nahda al-Arabiya for Printing, Publishing, 368.

- Teh, P.L, Ahmed, P. K. & D'arcy, J. (2015). ***What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory***. **Journal of Global Information Management** 23(1), 44–64**.**

- Tekleab, A.G. & Chiaburu, D.S. (2011). **Social Exchange, Empirical Examination of Form and Focus**, Journal of Business Research, *64*, 5, 462.

- Tenenhaus, M., Vinzi, V. E., Chatelin, Y. -M., & Lauro, C. (2005**). PLS Path Modeling.** Computational Statistics and Data Analysis, *48*(1), 159–205.

- Vance, A., & Siponen, M. (2012). ***IS security policy violations: A rational choice perspective.*** **Journal of Organizational and End User Computing** *24*(1), 21–41.

- von Solms, R., & von Solms, S. H. (2006). **Information Security Governance: A model based on the Direct–Control Cycle.** Computers & Security, 25(6), 408-412.

- Wetzels, M., Odekerken-Schröder, G., & Van Oppen, C. (2009). **Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration**. Management Information Systems Quarterly, 33(1), 177-195.

- Wold, H. O. A. (1982). **Soft modeling: The basic design and some extensions.** In K. G. Jöreskog & H. Wold (Eds.), Systems under indirect observations: Amsterdam: North-Holland.154.

- Zacher, H., Frese, M. (2009). **Remaining time and opportunities at work: Relationships between age, work characteristics, and occupational future time perspective**, Psychology and Aging, *24*, 487-493.

- Zhang, L. (2006). **Thinking Styles and the Big Five Personality Traits Revisited.** Personality and Individual Differences, *40*(179), 1177-1187.

- Zumrah, A.R. (2014). **Service Quality in Malaysian Public Sector: The Role of Transfer of Training**, 5th Asia-Euro Conference in Tourism, Hospitality& Gastronomy, *Procedia Social and Behavioral Sciences*, 144, 115.

Appendices

Appendix (1)

English Questionnaire

Dear Participant,

The researcher aimed to explore the impact of one's personal and professional characteristics on his/her compliance with information security policies. He aimed to explore that in order to fulfil the requirements of the master's degree in engineering management at Al-Najah National University. The present study sheds a light on five factors. Such factors include: individual and organizational factors. They also include factors related to work, workplace environment and compliance with information security policies. Information security refers to the protection of one's data or information against loss, theft, and fraud. The researcher believes that you are the best ones who will provide him with the required data. In order to conduct the present study, please fill in the questionnaire form. Filling it doesn't require more than 10 minutes. Please provide your answers in an objective manner. There aren't right or wrong answers. The data you will provide will be used for scientific research-related goals. Your workplace will not be disclosed.

Thank you for your cooperation in conducting scientific research

The researcher,

Bara' Abu Ja'far

The first part: Personal Information:

Gender:

□ Male □ Female

Age:

□ 18-38 years

□ 39-58 years

□ 59 years or more

Academic qualification:

□ Less than secondary school certificate

□ Secondary school certificate

□ Diploma degree

□ BA degree

□ Graduate degree

Marital status:

□ Single

□ Married

Major: ----------

Address: ----------

The current workplace: ----------

Job title:

□ Director □ Head of a department

□ Supervisor □ IT employee

□ Other

Years of experience in the field of information security:

□ Less than 10 years □ 11-20 years

□ 21 years of more

If you have a work experience certificate, please mention them: ----------

<u>The second part</u>: Exploring factors:

	No.	Statement	Attitude				
			Strongly agree	Agree	Neutral	Disagree	Strongly disagree
	First	**Individual factors**					
Neuroticism	1	I don't feel afraid nor stressed while working through using a computer					
	2	I don't feel that my value is lower than the value of my work colleagues					
	3	I don't feel that I will have a nervous breakdown while working under a huge pressure					
	4	I don't feel angry about the way I am treated					
	5	I don't have a pessimistic view towards life					
	6	I don't feel sometimes depressed and helpless.					
Extraversion	7	People perceive me as a cheerful, and active person who is full of energy					
	8	I respond to jokes and smile fast					
	9	I enjoy talking to people					
	10	I love being friendly and nice with others					
	11	I have a broad social relationship network					
	12	I love going to malls. I like the colors, lights and the crowds at malls.					
Openness	13	I am keen to illustrate my opinion					
	14	Using imagination and meditation participates in organizing time					
	15	I love travelling and visiting new places					
	16	I see beauty in the things that people perceive as being ordinary					
	17	I enjoy reading books and periodicals					

	18	I highly enjoy reading journals, and magazines, and surfing social media websites.					
Agreeableness	**19**	I highly believe that my work colleagues have good intentions					
	20	I exert much effort in order to meet my goals					
	21	I help my work colleagues much					
	22	I don't like hurting others' feelings					
	23	I carry out my work tasks accurately and efficiently					
	24	I forgive the ones who did a disservice to me					
Conscientiousness	**25**	I seek organizing my stuff and ensuring that they are clean.					
	26	I seek showing compliance with the institution's bylaw					
	27	I keep working - without stopping - till I finish my work					
	28	If things went bad, I don't feel desperate					
	29	I seek finishing my works before the due time and without receiving help from anyone.					
	30	People depend much on me. They trust me much					
Moral	**31**	I protect the institution's assets, including the institution's devices and apparatus					
	32	When there is a problem at work, I exert effort to solve it instantly					
	33	I am ready to handle the responsibility for my wrong acts					
	34	I highly respect my work colleagues and I don't like talking about them					
	35	I refrain from disclosing classified information to other institutions					

	36	I search for methods and means that can improve my work performance					
	Second	**Factors that affect employee satisfaction**					
Employee satisfaction	**37**	I am satisfied with my current basic salary when comparing it with the amount of tasks and responsibilities that I must handle					
	38	My job security level in the institution I work at is high					
	39	My direct supervisor deals in a fair manner with me					
	40	The moral incentives that I receive from my direct supervisor increase my productivity					
	41	I go in a bad mood in case I committed a fault that represents noncompliance with the institution's policies					
	42	I highly believe that the institution I work at retains the outstanding employees					
	Third	**Organizational factors**					
Support	**43**	If I faced a problem, I receive support from the institution's management					
	44	If I faced a problem, I receive support from my work colleagues					
	45	The institution's management seeks ensuring that the employees understand the goals.					
	46	Periodical reports are delivered about the extent of meeting the goals					
	47	I feel that my contribution to the institution are valuable and significant					
	48	I receive adequate attention from the institution's management					
Training	**49**	I am provided with the needed training that enables me to meet my professional needs					

	50	I receive the needed training about the information security policies					
	51	The training I receive enables me to improve my professional skills					
	52	The institution's management provides employees with training regularly					
	53	I receive theoretical and practical training					
	54	I receive training courses that suit my institutional position					
Culture	**55**	My institution provides much attention to the aspects related to the employee's personality. That is because the institution's management believes that all the employees are a big family					
	56	The institution's management seeks establishing an innovative culture					
	57	The institutional culture of my institution participates in building stable relationships between employees					
	58	The institution's management of my institution encourages employees to excel at work					
	59	The institutional culture of my institution participates in meeting the goals and raising productivity					
	60	The institution's management of my institution seeks developing human resources					
	Fourth	**The workplace environment (the availability of appropriate conditions and apparatus)**					
Technological Work Environment	**61**	The institution has programs for protecting all its devices. These programs uploaded in a regular manner					
	62	The institution's communication channels are characterized with transferring information smoothly					

	63	The workplace is well-lit					
	64	The workplace includes office supplies and great decorations					
	65	There are modern and advanced devices at the workplace					
	66	The availability of air condition devices in my office enables me to focus in work					
	67	The workplace is characterized with being far away from the city center and noise					
	Fifth	**Compliance with the information security policies**					
Compliance	**68**	I believe that practicing my profession requires acknowledging the institution's bylaws, regulations, and instructions.					
	69	The policies and procedures related to information access are clear					
	70	All the employees acknowledge the information security policy. There has been an agreement reached on the latter policy					
	71	The password that I use consists from a mixture of words, numbers, and letters					
	72	When going on a break or to the bathroom, I shutdown my computer					
	73	I don't download files from websites that are not well-known					
	74	I instantly report any bug gets detected in the system					
	75	I protect my personal information. I consider protecting such information as something important					

	76	When using my institution's devices, I don't use a wireless network of any other institution					
	77	I make backup copies for the important files					
	78	I don't use the social network websites while working					

Appendix (2)

The Arabic version of the questionnaire

المشترك الكريم/ة:

يسعى الباحث في هذه الاستبانة الى دراسة تأثير السمات الشخصية والمهنية في الالتزام بسياسات امن المعلومات وذلك استكمالا لمتطلبات الحصول على درجة الماجستير في الادارة الهندسية من كلية الدراسات العليا في جامعة النجاح الوطنية حيث تتضمن الدراسة خمسة عوامل رئيسية : العوامل الفردية ،عوامل العمل ، العوامل التنظيمية، بيئة العمل وسياسات الالتزام بأمن المعلومات. حيث ان امن المعلومات هو الحفاظ على بياناتك او معلوماتك من الضياع او السرقة او الاحتيال . ونحن نعتقد انكم افضل من سيزودنا بالمعلومات اللازمة لتنفيذ هذه الدراسة من خلال تكرمكم بتعبئة هذه الاستبانة التي لا تستغرق اكثر من 10دقائق والإجابة عليها بكل موضوعية، علمًا أنه لا توجد إجابة صحيحة أو خاطئة وسوف تستخدم المعلومات الواردة فيهما لأغراض البحث العلمي فقط ولن يتم الافصاح عن مكان العمل .

شاكرين لكم حسن تعاونكم لخدمة البحث العلمي.

الباحث

براء ابو جعفر

القسم الاول : المعلومات الشخصية :

الجنس : ☐ ذكر ☐ أنثى

العمر: ☐ 18-38 ☐ 39-58 ☐ 59 فأكثر

المستوى التعليمي: ☐ أقل من ثانوية عامة ☐ ثانوية عامة ☐ دبلوم متوسط
☐ بكالوريوس ☐ دراسات عليا

الحالة الاجتماعية : ☐ اعزب ☐ متزوج

التخصص:_____

مكان السكن:_____

مكان العمل:_____

المسمى الوظيفي: ☐ مدير ☐ رئيس قسم ☐ مشرف
☐ موظف IT ☐ موظف ☐ غير ذلك

سنوات الخبرة في مجال امن المعلومات : ☐ اقل من 10 سنوات ☐ من 11-20 سنة
☐ 21 سنة فأكثر

شهادات خبرة في مجال امن المعلومات ان وجد :_____

القسم الثاني: دراسة العوامل

	الرقم	الفقرة	درجة الاستجابة				
			اوافق بشدة	اوافق	محايد	لا اوافق	لا اوافق بشدة
	اولا	**العوامل الفردية**					
العصبية	1	ليس لدي شعور بالقلق والخوف أثناء عملي أمام الحاسوب					
	2	لا أشعر بأني اقل مستوى من زملائي بالعمل .					
	3	لا أشعر بأن أعصابي سوف تنهار تحت الضغط الهائل.					
	4	لا أشعر بالغضب من الطريقة التي أعامل بها.					
	5	لا انظر الى الحياة بتشاؤم.					
	6	لا أشعر أحيانا بالكآبة والعجز					
الانبساط	7	يصفني الاخرون بأني شخصية مرحة ومليئة بالحيوية والنشاط.					
	8	أستجيب بسهولة للنكتة وابتسم سريعا.					
	9	أشعر بالمتعة عند الحديث مع الآخرين.					
	10	أحب أن أكون ودودا ولطيفا مع الاخرين.					
	11	علاقاتي الاجتماعية واسعة وكبيرة					
	12	أحب كثيرا الذهاب الى مراكز التسوق بما فيها من ألوان وأضواء وازدحام.					
الانفتاح	13	أحرص على توضيح وجهة نظري					
	14	اللجوء للخيال والتأمل ينظم الوقت					
	15	أفضل السفر وزيارة أماكن جديدة.					
	16	أرى الجمال في أشياء قد يصفها الآخرون انها عادية .					
	17	أستمتع كثيرا في القراءة والمطالعة للكتب والدوريات					
	18	أستمتع كثيرا في قراءة ومطالعة الجرائد والمجلات ووسائل التواصل الاجتماعي					
الطيبة	19	اثق في نوايا زملائي.					
	20	أجتهد بكل قوتي من أجل إنجاز وتحقيق أهدافي.					
	الرقم	الفقرة	اوافق بشدة	اوافق	محايد	لا اوافق	لا اوافق بشدة
	21	أساعد زملائي في العمل كثيرا					
	22	لا احب ابدا جرح مشاعر الآخرين.					
	23	اقوم بإنجاز أعمالي بإتقان ودقة وكفاءة.					
	24	أعفو عن من اعتدى علي من زملائي.					
الضمير	25	أسعى إلى ترتيب أشيائي وان تكون نظيفة وفي مكانها.					
	26	أحرص بشدة على ان اكون ملتزماً بالنظام.					
	27	اواصل عملي ولا أتركه حتى أنهيه.					
	28	لا أتعب ولا أشعر بالكلل والفتور إذا سارت الأمور نحو الأسوأ.					
	29	أسعى لتأدية أعمالي في الوقت المحدد لها وبدون مساعدة.					

	30	يعتمد على الاخرون كثيرا و يوثقون بي.							
اخلاقيات العمل	31	اقوم بالمحافظة على اصول الشركة من اجهزة وادوات.							
	32	عند وجود مشكلة في العمل فاني اعمل على حل المشكلة في نفس اللحظة.							
	33	لدي الاستعداد لتحمل المسؤولية الناتجة عن تصرفاتي الخاطئة.							
	34	احترم كثيرا زملائي في العمل ولا احب الحديث عنهم							
	35	التزم بعدم اعطاء معلومات سرية للمؤسسة للأخرين .							
	36	أبحث عن طرق ووسائل لتحسين عملي.							
	ثانيا	**العوامل المساعدة على رضى الموظفين**							
رضى الموظفين	37	يعتبر الر اتب الأساسي الحالي الذي أتقاضاه مقارنة بحجم مهامي ومسئولياتي داخل العمل مرضيا لي.							
	38	أشعر بالأمان الوظيفي في مؤسستي.							
	39	مديري المباشر يتعامل معي بعدالة .							
	40	التحفيز غير المادي من قبل مديري يزيد من إنتاجيتي.							
	41	يتعكر مزاجي في حال تعرضت لخلل في تطبيق سياسات الشركة.							
	42	لدي الثقة بان المؤسسة تحافظ على الموظفين المتميزين بالعمل							
	الرقم	الفقرة	اوافق بشدة	اوافق	محايد	لا اوافق	لا اوافق بشدة		
	ثالثا	**العوامل التنظيمية**							
الدعم	43	اتلقى الدعم من ادارة المؤسسة في حال واجهتني مشكلة معينة							
	44	اتلقى الدعم من زملائي في العمل في حال واجهتني مشكلة معينة							
	45	يتم التعاون من قبل المؤسسة في فهم اهداف العمل							
	46	يتم رفع تقارير دورية بخصوص انجاز الاهداف							
	47	أشعر ان مساهمتي في المؤسسة كبيرة ومهمة							
	48	أتلقى الاهتمام الكافي من قبل المؤسسة .							
التدريب	49	يتم تزويدي بالتدريب المطلوب لاحتياجاتك الوظيفية							
	50	اتلقى التدريب اللازم بخصوص سياسات امن المعلومات.							
	51	يعمل التدريب على تحسين وتطوير مهاراتي في العمل							
	52	يتم عمل تدريب بشكل دوري للموظفين في المؤسسة							
	53	أتلقى التدريب بشكل نظري وعملي							
	54	اتلقى تدريب مناسب لموقعي التنظيمي							

الثقافة	55	تهتم مؤسستي بالجوانب الشخصية للموظف فهي بمثابة عائلة كبيرة						
	56	تقوم مؤسستي بتشجيع الافراد على ثقافة الابداع						
	57	ثقافة المؤسسة التي اعمل بها تساعد على استقرار العلاقات بين الموظفين						
	58	تشجع ادارة المؤسسة على التميز في العمل						
	59	تساعد ثقافة المؤسسة على زيادة الانتاج وتحقيق الاهداف						
	60	تسعى مؤسستي على تطوير الموارد البشرية						
	الرقم	الفقرة	اوافق بشدة	اوافق	محايد	لا اوافق	لا اوافق بشدة	
	رابعا	**بيئة العمل (توفر الظروف والادوات المناسبة)**						
التكنلوجية	61	يتوفر برامج حماية في جميع اجهزة المؤسسة ويتم تحديثها بشكل دوري						
	62	قنوات الاتصال بالمؤسسة ذات انسيابية في نقل المعلومات والقرارات						
	63	يتميز مكان العمل بإضاءة جيدة						
	64	يتميز مكان العمل بتجهيزات مكتبية وديكور رائع						
	65	يستخدم اجهزة حديثة ومتطورة في مكان العمل						
	66	توفر اجهزة التكييف في المكتب يساعدني على التركيز في العمل						
	67	يتميز مكان العمل ببعده عن مركز المدينة وعن الضوضاء						
	خامسا	**الالتزام بسياسات امن المعلومات**						
الالتزام	68	أؤمن بأن عملي مهنة تعتمد على الأنظمة والقوانين والتعليمات في المؤسسة.						
	69	سياسات واجراءات صلاحيات الدخول للمعلومات واضحة						
	70	سياسة امن المعلومات معروفة لدى الموظفين وتمت الموافقة عليها						
	71	استخدم كلمة مرور خليط من احرف وارقام ورموز						
	72	اقوم بأغلاق جهاز العمل عند الذهاب للاستراحة او الحمام						
	73	لا اقوم بعمل تنزيل ملفات من مواقع الكترونية غير معروفة						
	74	اقوم بالتبليغ عن أي نقطة ضعف امنية تم اكتشافها فورا						
	75	احافظ على معلوماتي الشخصية واعتبر ان حمايتها مهمة						
	76	لا استخدم أي شبكة لا سلكية من خارج العمل على اجهزة المؤسسة						
	77	اقوم بعمل نسخ احتياطي للملفات المهمة						
	78	لا استخدم شبكات التواصل الاجتماعي اثناء العمل						

Appendix (3)

Arbitrators

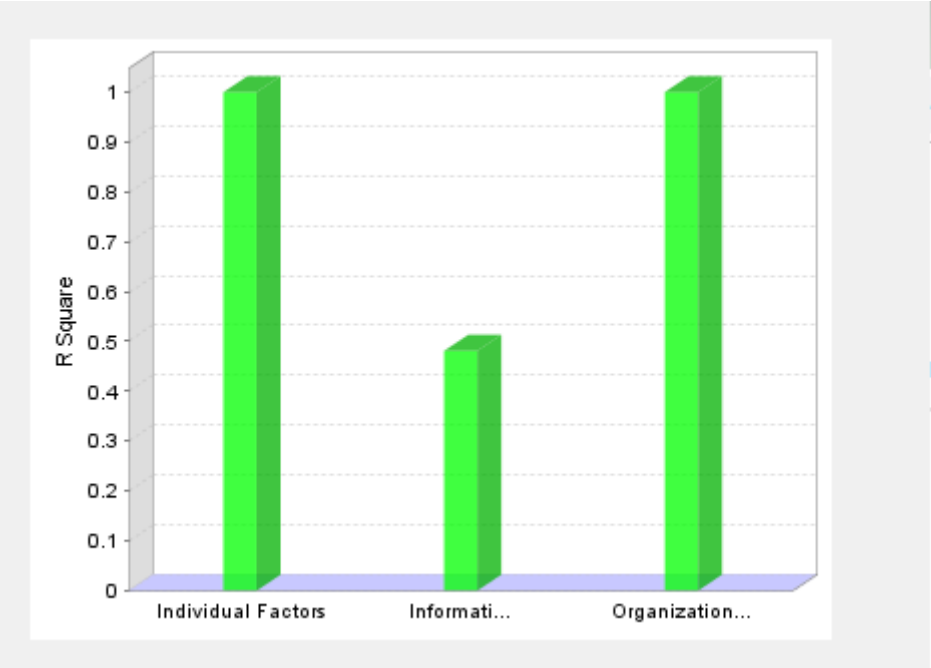
Name:	Specialization	Position
Dr. Ahmad Awad	Communications and Computer Engineering	Assistant Professor at Department of Computer Science at An - Najah National University.
Dr. Suhel Salhaa	Curriculum and Instruction	Head of Department of Upper Elementary School Teacher
Dr. Yahya Saleh	Industrial Engineering and Operations Research	Director of the Success Center for Innovation and Partnership
Dr. Ayob Abed Alkareem	Measurement and Evaluation	Assistant Professor at Department of Educational Sciences An - Najah National University

Appendix (4)

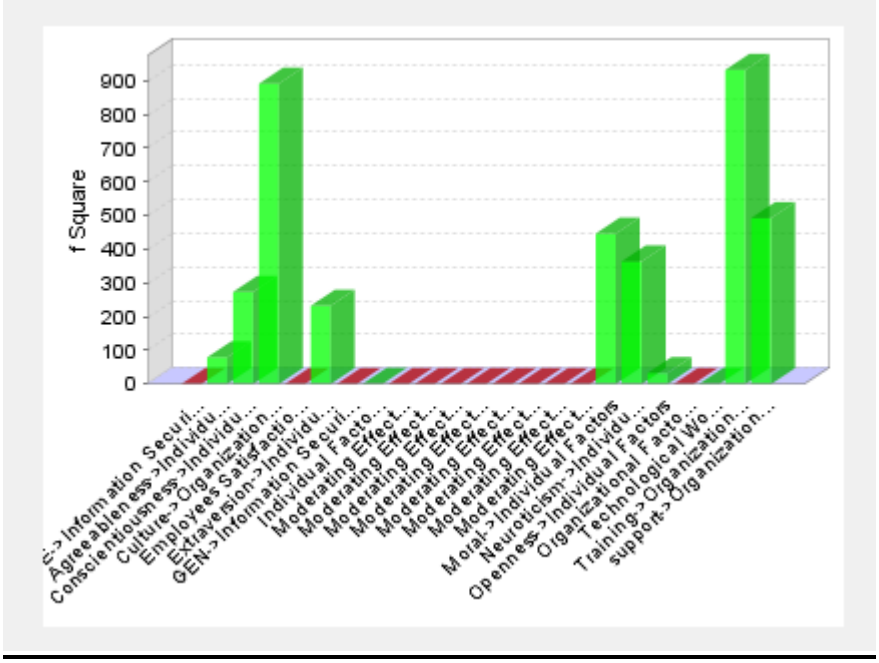
Simple Slope Analysis charts

Quality Criteria

1- R Square

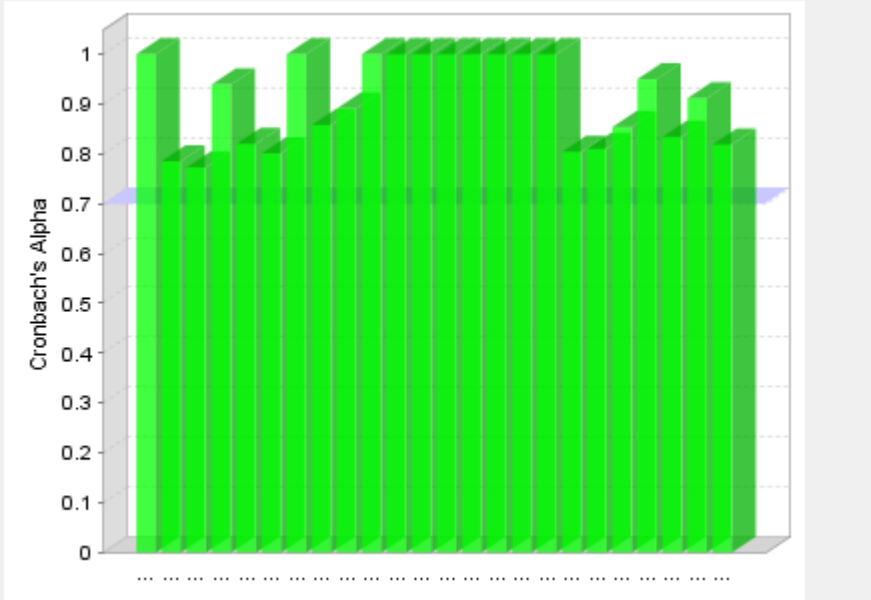


2- f Square



3- Construct Reliability and Validity charts

Cronbach's Alpha

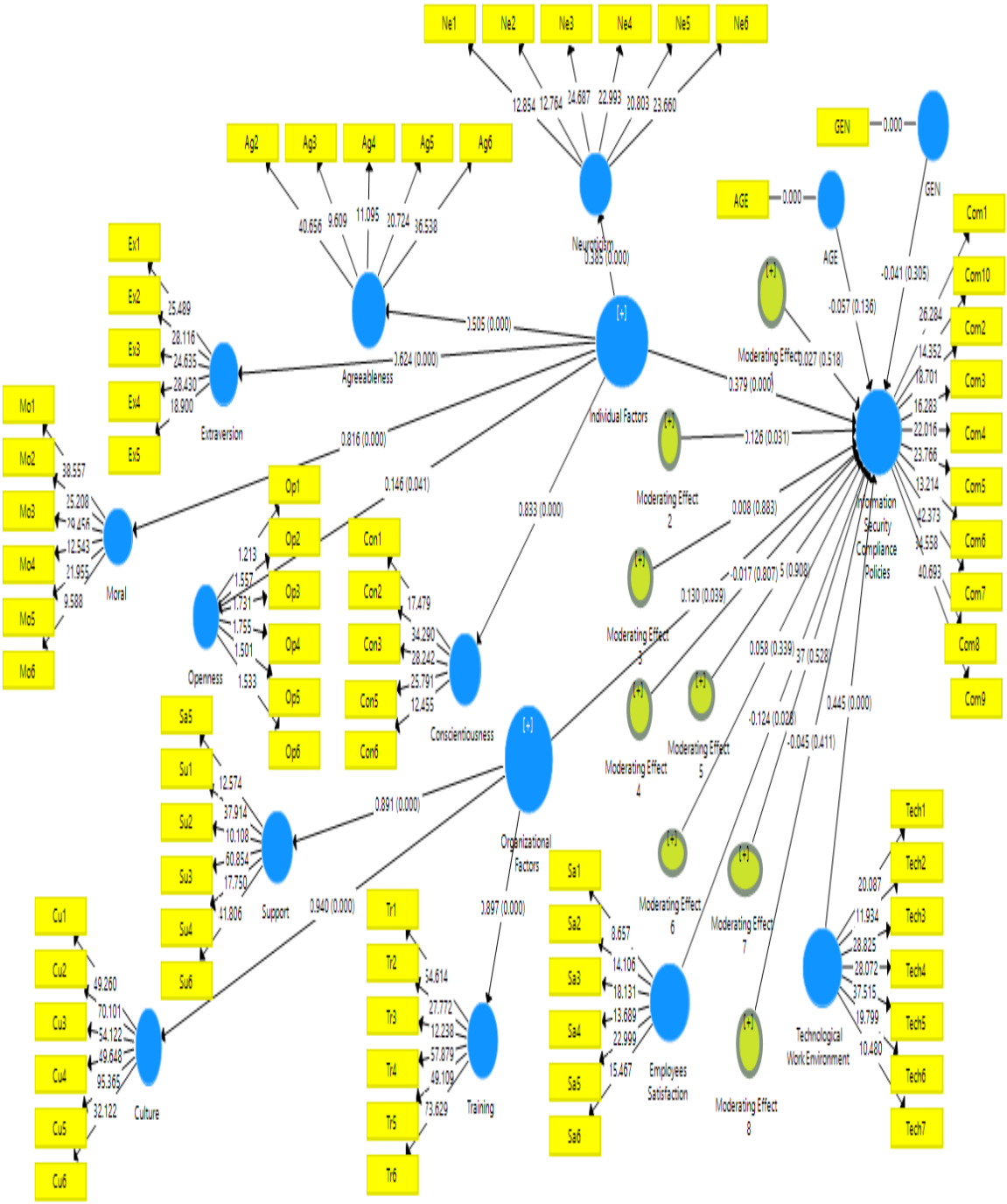


Composite Reliability

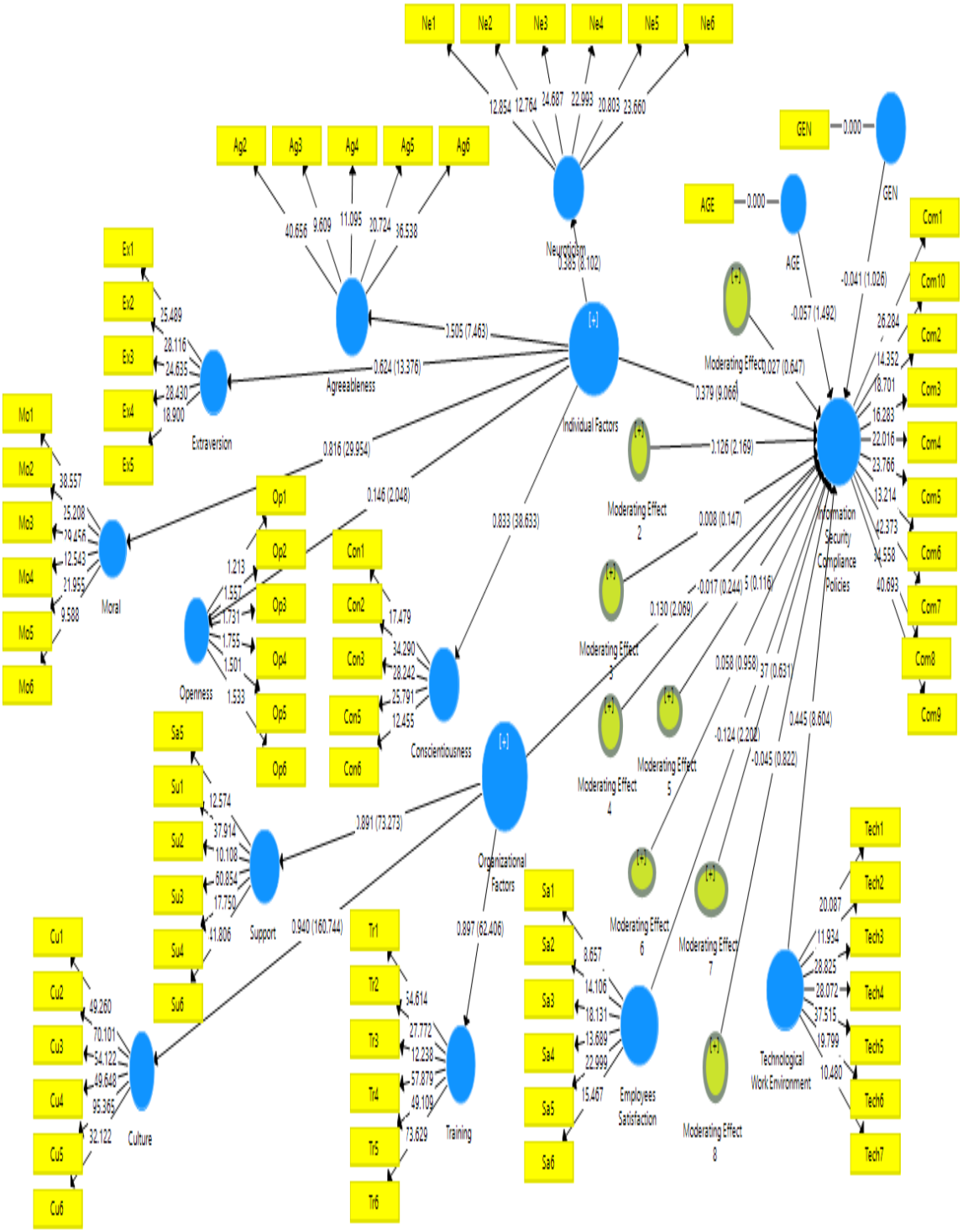
Appendix (5)

Measurement and Structural Model Results

1- model (path coefficients and P value)



2- model (path coefficients and T value)



جامعة النجاح الوطنية

كلية الدراسات العليا

العوامل المؤثرة في الموظفين على الامتثال لسياسات أمن المعلومات في فلسطين

اعداد

براء ابو جعفر

اشراف

د. محمد عثمان

د. عبد الفتاح ملاح

قدمت هذه الاطروحة استكمالاً لمتطلبات الحصول على درجة الماجستير في الإدارة الهندسية، بكلية الدراسات العليا، في جامعة النجاح الوطنية، نابلس– فلسطين.

2019

العوامل المؤثرة في الموظفين على الامتثال لسياسات أمن المعلومات في فلسطين

اعداد

براء ابو جعفر

اشراف

د. محمد عثمان

د. عبد الفتاح ملاح

الملخص

أمن المعلومات مهم للغاية للمؤسسات والهيئات، حيث يمثل الخطأ البشري أكبر تهديد لأمن المعلومات. لذلك يتعين على المؤسسات تطوير وتحسين أداء الموظفين للالتزام بسياسات أمن المعلومات. الهدف من هذه الرسالة هو دراسة العوامل المحتملة التي تؤثر على امتثال الموظفين لسياسة أمن المعلومات. لذلك، طبيعة هذه الدراسة تأخذ طبيعة التحليل الاستكشافي. الفئة المستهدفة للدراسة هي الموظفين بشكل عام في فلسطين الذين يستخدمون أجهزة الحاسوب أثناء عملهم. لذلك، تم توزيع 500 استبيان على العينة المستهدفة، ولكن 372 استبانة فقط كانت صالحة للتحليل، مع معدل استجابة 74.4 ٪. وقد تم توزيع العينة على العديد من المؤسسات الخدماتية بما في ذلك الجامعات وشركات الاتصالات ومزودي خدمات الإنترنت وشركات التأمين والبنوك. باستخدام طريقة المربعات الصغرى الجزئية، أشارت النتائج إلى أن العوامل الشخصية للموظفين ، والعوامل التنظيمية، وبيئة العمل التكنولوجي بالإضافة الى العوامل البيئية الاخرى لها تأثير إيجابي على الامتثال لسياسات أمن المعلومات. أيضا، تظهر النتائج أن الموظفين الأكبر سنا يميلون إلى الامتثال لسياسات أمن المعلومات اكثر من الموظفين الاصغر سنا في جميع مراحل العمل داخل المؤسسة. علاوة على ذلك، ليس لجنس الموظف ذكر او انثى أي تأثير كبير على سياسات الامتثال لأمن المعلومات. هذه النتائج مفيدة لصانعي السياسات في المؤسسات الذين يخططون لتحسين امتثال الموظفين لسياسات أمن المعلومات، والباحثين المهتمين بهذا المجال. تم اقتراح بعض التوصيات لمديري المؤسسات مثل: زيادة الدعم المؤسسي للموظفين، وإجراء تدريب دوري على أمن المعلومات، ونشر الإبداع والتميز بين الموظفين، وتوفير بيئة مناسبة وجيدة للموظفين.