Empirical Study to Analyse Information Security Awareness of NUST Students

By

Tanzeela Younas Malik

NUST201464172MSEECS63114F

Supervisor

Dr. Seemab Latif

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS IS)

In

School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(May, 2018)


بسم الله الرحمن الرحيم
١٤١٨

Approval

It is certified that the contents and form of the thesis entitled "**Empirical Study to Analyse Information Security Awareness of NUST Students**" submitted by **Tanzeela Younas Malik** have been found satisfactory for the requirement of the degree.

Advisor: **Dr. Seemab Latif**
Signature:_____

Date:_____

Committee Member 1: **Dr. Syed Taha Ali**
Signature:_____
Date:_____
Committee Member 2: **Dr. Hassan Tahir**
Signature:_____
Date:_____
Committee Member 3: **Miss Haleemah Zia**
Signature:_____
Date:_____

Dedicated
to
my beloved Parents!

Certificate of Originality

I hereby declare that this submission titled **Empirical Study to Analyse Information Security Awareness of NUST Students** is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged. I also verified the originality of contents through plagiarism software.

Author Name: **Tanzeela Younas Malik**
Signature:_____

Acknowledgment

First of all, I would THANKS to ALLAH ALMIGHTY for helping me in completion of master's degree. By the grace of ALLAH, I am able to accomplish this goal in my life with full dedication and motivation. After that, Special Thanks to my precious parents for their everlasting love and too much support throughout my thesis phase. Special thanks to my lovely sisters for always being there, whenever I need them to share my thoughts and specially for gossiping sessions. I would like to Appreciate my Khala and nani for their prayers and never-ending support. I would like to thanks my supervisor Dr. Seemab Latif who has always inspired me with her dedication and enthusiasm to work. Her guidance, motivation and mentorship by far had been the most encouraging factors to complete my research work. I would like to appreciate and thank my committee members, Dr. Hassan Tahir, Dr. Syed Taha Ali and Miss Haleemah Zia who had always given me their precious time and guided me through my thesis work. Their critique has always helped me in improving my work.

I would like to especially thanks Miss Haleemah Zia who has provided me all kind of help and encouragement in my thesis work. Bundle of thanks to Miss Haleemah Zia for helping me in implementation phase as well.

Tanzeela Younas Malik

Table of Contents

List of Figures

List of Tables

Abstract

Every aspect of information security cannot be addressed efficiently by taking only technical measures into consideration. With the increasing rate of insider threat, information security awareness plays a crucial role in fulfilling security requirements of an organization. The main aim of the study is to examine the relationship between individual, environmental, cultural factors and information security awareness (ISA). This quantitative study has used the primary data collected from twin cities of Pakistan including Rawalpindi and Islamabad by targeting the university students having sample size of (N=501) students. Personality traits have been found as an important factor in user behavior towards security. This study incorporates the personality traits as individual factor, peer pressure and secondary source influence as environmental factor, rule following as a cultural factor of an organization in theoretical framework to investigate their impact on students' ISA. Openness and environmental factors have shown positive impact on ISA. Cultural factor shown strong but negative impact on ISA due to openness personality of the target audience. On the basis of the statistical analysis, we incorporated the new components in the NIST awareness program framework to fill the gap of improving user behavior towards information security. This framework would fulfill the demands of tailored awareness program which could not only improve knowledge but behavior as well by catering the environmental, cultural and individual aspects.

CHAPTER 1

Introduction

Chapter 1 of the presented thesis provides comprehensive overview of our thesis work which is based on the domain of information security awareness in education sector. This chapter elaborates the roadmap of thesis and highlights the further organization and structure of the thesis. This chapter also explains the aim for carrying out the research work. Eventually the chapter highlights the goals of each following chapter to represent the overall thesis organization.

1.1 Information Security Awareness

With the advent of information technology, organizations have become highly dependent on information processing. Due to the increasing rates of threats to information, information security has become an important factor for the success of an organization, thereby, translating into a major challenge for organizations today (Aurigemma and Panko 2012; Chan and Mubarak 2012).

Information security preserves the Confidentiality, Integrity and Availability (CIA) of information. It prevents unauthorized access, disclosure, disruption, modification, inspection or destruction of information (Laudon and Laudon, 2010). It has both technical and non-technical aspects but organizations mostly emphasize on the former. Technical measures alone, however, are considered insufficient as the user himself/herself is unaware of security issues, policies and practices (Chan and Mubarak 2012). Earlier research has focused mainly on technical measures such as firewall and encryption etc. However, majority of the mishaps regarding information security breaches in organizations result from users' own mistakes (Siponen and Vance, 2010). According to IBM 2016 Cyber Security Intelligence Index, 90% of the security incidents involve human error. This makes it ever more important to take the human factor into consideration as it poses a serious threat to information security. Various surveys have revealed that inside breaches have increased up to 75% with devastating effects on the wellbeing of the organization, with 50% caused by inadvertent human error, being not only difficult to detect but also to correct (Information Security Breaches Survey 2015; 2016 Cyber Security Intelligence Index).

Advancement in technology and its use has led to drastic increase in information security risks. In an internet security threat reported by Norton, in 2015 over one million web attacks were launched by cybercriminals against internet users every day. Security hazards like identity theft, user surveillance, phishing, viruses and stolen passwords are some of the risks that are ever-existent to users' information (Jeske and van Schaik, 2017). Attacks linked to such security risks are not restricted to any particular faction of the population but have affected all types of users

including professionals, teachers, students and parents (Byron, 2008). In this era of staying online 24/7, millennials tend to be the most vulnerable to internet crime. They seem less conscious about security and pay less attention to their personal security as reported by Norton cyber security. Students are considered as an important group of users which needs to be investigated in terms of information security (Van Schaik *et.al.*, 2017). Vast computing power enables users to have open access to information and adopt IT at high rates, thereby, increasing the risk of security breaches (Muhirwe and White, 2016). According to the report by Identity Theft Resource Center (mid-year 2016), 11.3% of the total breaches originated in the educational sector indicating it as a hot target for security attacks.

Increased rate of breaches by humans is considered one of the main reasons behind the attention that the IT industry pays to information security awareness. The purpose of Information Security Awareness (ISA), according to NIST SP 800-16, is *"not training*". Rather, awareness presentations mainly aim to *"focus attention on security…to allow individuals to recognize IT security concerns and respond accordingly".* Security awareness, a subset of information security, is still in its evolution phase, focusing primarily on raising consciousness regarding risks and threats to information. Kruger & Kearney, 2006 classified ISA into three dimensions: Knowledge, Attitude and Behavior, as shown in Figure 1. The behavioral dimension of information security awareness is an interdisciplinary domain taking theories from psychology and criminology. A theory based literature review was conducted by Lebek *et.al.,* in 2013 which reviewed the underlying applied theories used to analyse employee information security awareness and behaviour. There, however, remains the need for a comprehensive review of information security awareness in educational institutes as the careless attitude of students towards security and their lack of privacy make them a much more vulnerable part of the community (van Schaik *et.al.*, 2017; Tan and Aguilar, 2012). These students are future employees and thereby an integral part of different organizations and their careless behavior and lack of knowledge about security poses serious risks to the security health of these organizations (Muhirwe and White, 2016; van Schaik *et.al.*, 2017).

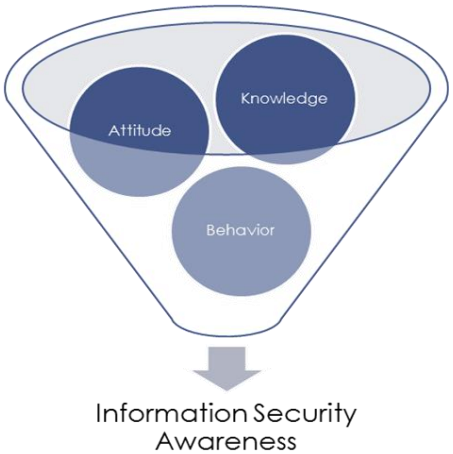


Figure 1.1 Dimension of Information Security Awareness (Kruger & Kearney, 2006)

The aim of this study is to identify the deficiencies in assessing security awareness and in frameworks designed for improving awareness in an organization. It also enhances the researcher's knowledge and helps him/her in developing better assessment strategies, at the same time, increasing information security awareness in the education sector. Analysing different factors helped in countering the deficiencies found in existing awareness program frameworks. The improved framework would be helpful in improving the awareness programs, thus, enabling organizations to change user perception and behaviour towards the secure use of technology. Organizations could personalize their awareness programs according to the target set of users to establish a more effective program.

1.2 Aims and Scope

Organizations are competing in the information technology world to keep their digital assets secure from the financial and reputational damage. Organizations are striving for prevention from these threats. One of the biggest threats to assets is humans. Security awareness and training programs are one of the effective techniques for securing the organizations from the intentional and unintentional malicious insiders. With increase in such threats in last decade as mention in introductions section, our project aims to help research community and management of organizations to improve their security awareness programs. This would be achieved by making security awareness programs more effective through improving behavior of individuals towards security. Through our project two main objectives have been achieved:

- Review of literature highlighted the deficient analysis of combined effect of individual, environmental and cultural factors on ISA. Current solution considered the three dimensions effect on one's knowledge, attitude and behavior towards information security. This study also defined the variance of ISA levels among technical and non-technical students.
- Review of the literature helped in identifying the deficiencies and areas of improvement in awareness programs. Critical analysis revealed the need for comprehensive solution. A framework is proposed to bridge the major deficiencies identified in the literature. Ad hoc model of awareness program provided as a sample for other institutes to tailor programs according to their needs.

The purpose of this research was to provide a framework that not only increases their knowledge abut also influence their behavior towards information security. This framework provided a personalized view of awareness programs according to the audience which could be helpful in influencing them the most.

1.3 Limitations

In order to limit the extent of this work we have restricted our research from several aspects:

- Data collection was performed randomly from different institutes of NUST. Due to time constraint, the survey was conducted in ten institutes. We generalized the collected sample for the population.
- The ad hoc model for awareness program is only provided for one institute. The focus has been kept limited as for targeting each institute separately would require more sample, time and resources.
- Results would not be evident until we practically implement the framework which would require years of implementation and enforcement.
- The influential strategies would be more fruitful if it would be selected after taking feedback from the respective audience. The selectin of strategies has been mentioned in the Future work in Chapter 5.

1.4 Thesis Organization

This document consists of five chapters. Chapter 2 presents the systematic literature review which has been conducted throughout the research phase. It elaborates the strategies and frameworks used to design ISA programs for educational institutes. It also provided the comprehensive overview of the social and psychological factors used in literature. Chapter 3 presents the research methodology considered for this thesis which describes the different phases of the research. These phases outline the research process under different phases of research. Chapter 4 analyzed the results deduced after the data collection process. Results are as per hypothesis and the respective statistical analysis required for the evaluation. Chapter 5 concludes the study by improving the NIST awareness program framework according to analysis results in previous chapter. In this chapter we also provided the ad hoc model for one of the institutes of the selected organization to give a practical overview of the improved framework. In the Appendix section we provided the questionnaire used for data collection for this study.

Summary:

In this chapter, we have presented the brief overview of the introductory concepts and motivation behind this research work. It gives a comprehensive overview information security awareness concepts and the motivation to carry out the research work. Furthermore, the chapter presents main objectives and contributions of our research work, as well as overall thesis organization.

CHAPTER 2

Literature Review

This chapter focuses on the existing literature related to different factors and their effect on information security awareness. These factors are deducted from theories of psychology, health, criminology and behavioral sciences. This review identifies the approaches used to assess security awareness in organizations and educational institutes. It also demonstrates the factors that influence and motivate the security behavior. This chapter discusses information security awareness in education sector based on the guidelines proposed by Kitchenham et.al., 2009.

2.1 Information Security Awareness (ISA) in Educational Institutes

We have summarized the studies conducted in educational institutes in Table 2.1 according to different stakeholders considered by the study like students, academic and administrative staff. The assessment methods used for data collection were also summarized in the table. Outcomes of the studies in the form of recommendations of ISA training, focus on security policy or security education by making it part of curriculum were also highlighted in Table 2.1.

In information security awareness field, mostly authors used self-reported approach to assess the ISA level among users. Other methodologies included open-ended questions, scenario based questions, interviews, observations and documentation (Marks and Rezgui, 2009). In observation as assessment method, the respondent data was collected through observation of skills in practice. Assessment through documentation included review of existing records like log file analysis, monthly reports.

As defined by NIST SP 800-16, security awareness was designed to change behaviour and reinforce best practices. Behavioural information security as subfield of information security focuses on behaviours regarding information and asset protection. Behavioural theories have been applied to understand the human behaviour regarding asset use and protection measures like Email and internet use, computer abuse, performance of security measures, security policy compliance, incident reporting, information handling (Warkentin *et.al.,* 2012; Parsons *et.al.,* 2014; Da Veiga and Martins, 2015; Crossler *et.al.,* 2013).ISA research field uses theories from psychology, sociology and criminology. The most frequently used theories were Theory of Reasoned Action (TRA), General Deterrence Theory (GDT), Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), Social Cognitive Theory (SCT), Constructivism and Social Learning Theory (SLT) (Lebek *et.al.,* 2013; Warkentin *et.al.,* 2012).

The overlapping constructs from these underlying theories showed interdependence between awareness level and behavioural intent. These interrelated constructs addressed ‘knowing and doing’ gap and helped in getting reflection of actual behaviour. As only increasing awareness

Table 2.1 Literature Review Summary

			Chan et.al. 2012	Stanciu et.al. 2016	Ögütçü et.al. 2016	Ramalingam et.al. 2016	Ahlan et.al. 2015	Farooq et.al. 2015	Al-Janabi et.al. 2016	Ismailova et.al. 2016	Muhirwe et.al. 2016	Shropshire et.al. 2015	Kruger et.al. 2011	Warkentin et.al. 2016	Hamid et.al. 2014	Johnston et.al. 2012	Arachchilage et.al. 2014	Arpaci et.al. 2016	B.Kim, 2014	van Schaik et.al. 2017
Where study Applied	Academia	Staff Officer	✓		✓	✓	✓		✓							✓				
		Faculty	✓		✓	✓	✓		✓							✓				
		Students		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Factors	Demographics		✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓				✓	✓
	Behavioural	Big 5 Personality										✓								
		Behaviour	✓	✓	✓		✓	✓	✓	✓		✓	✓			✓	✓			
		Attitude		✓	✓		✓					✓				✓		✓	✓	
		Other*			✓		✓					✓		✓	✓		✓	✓		✓
	Environmental						✓											✓		
	Knowledge		✓			✓		✓	✓	✓			✓	✓	✓		✓		✓	✓
	Others **				✓		✓	✓		✓	✓		✓	✓		✓		✓		✓
Methods	Questionnaire		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
	Interviews														✓					
	Open-Ended Questions		✓							✓										
	Scenario Based Questions		✓					✓					✓							
Statistical Tests	ANOVA				✓			✓		✓			✓	✓		✓	✓		✓	✓
	Correlation Coefficient				✓		✓	✓	✓											
	Regression										✓	✓								
	T- Test			✓			✓					✓			✓					
	CFA																	✓		
	SEM										✓	✓						✓		
Research Outcomes	Training /Awareness		✓		✓	✓	✓	✓	✓		✓		✓	✓	✓		✓	✓	✓	✓
	Policy					✓	✓								✓				✓	
	Curriculum			✓						✓	✓									

*Risk taking propensity, Ability to control impulsivity, Conservative Behaviour, Risk perception, Self-Cognitive, Intention to comply, perceived ease of use, perceived usefulness, self-efficacy, response-efficacy, perceived severity, perceived vulnerability, perceived risk, perceived benefit, perception of risk dimensions, avoidance motivation, Intention to knowledge sharing

**Exposure to Offensive scale, Policy compliance, Working Experience, mother tongue, type of school attended, threat awareness, countermeasure awareness, response cost, risk balance, computer security use, internet experience, source trustworthiness, source dynamism, source competency

could not address the ISA goals without changing behavior toward security practices (Ngoqo and Flowerday, 2014).

Changing behaviour toward information security is a challenging task as it requires first the relevant knowledge, then willingness to apply the advice (attitude) which shows effects in tasks they actually perform (behaviour) (Bada and Sasse, 2014). Human behaviour considered as the cause of increased security breaches. The awareness level and behavioural intent both could be improved by focusing on the factors which in turn influenced the relationship between level of awareness and behavioural intent. Such factors include attitude, subjective norms and perceived behavioural control interdependence etc. which have influential effects on actual security behaviour (Ngoqo and Flowerday, 2014).

Information security awareness can be the insight of user's knowledge of security concepts, user awareness or consciousness of organizational policies. The lack of awareness reflects in user's behaviours (e.g. password sharing) which results due to lack of policy promotion and its enforcement in organizations. By analysing the relationship between conceptual knowledge and behaviour, organizations can identify the focus area as per their organization environment which highlight the risks as well (Chan and Mubarak, 2012; Ismailova and Muhametjanova 2016). Chan and Mubarak, 2012 found lack of knowledge of concepts in academic and administrative staff of higher education. The employee did not have any knowledge about the existence of organizations' security policies. Their observations showed that employees who have the knowledge of phishing and strong password still engaged in clicking of potential spam links as well as in password sharing. They recommended security awareness to be part of risk assessment strategies to mitigate risks. Organizations require proper risk assessment which could mitigate the risks by adopting relevant awareness program. These programs will help in developing security compliance culture in an organization. The relationship of security risk assessment and security awareness was also evident in a study by Mejias, 2012. They identified three constructs i.e. technical knowledge, organizational impact and attacker assessment to provide integrative perspective of ISA, malicious IT and ISA association with risk assessment. Through empirical study, they found that organizational impact and attacker assessment had stronger correlation with ISA than technical knowledge. A strong correlation between ISA and information system security risk assessment was observed, which revealed that as organizations have more knowledge of malicious IT, the better their risk assessment will be.

Many studies recommended awareness and training programs as a solution after analysing individuals ISA level and their security behaviour in organizations (Al-Janabi and Al-Shourbaji, 2016; Da Veiga and Martins, 2015). Training and awareness programs positively influence an organization's information security culture. Through continuous improvement in such trainings, the IS culture of organization will direct employees towards compliance and regulatory requirements (Da Veiga and Martins, 2015). McBride *et.al.,* (2012), highlighted the need of customized training protocols. Individuals with different personality traits need training programs per their personality. As individuals with diverse personality perform differently in

same situations so they need to get training as per personality. They suggested three levels of cybersecurity trainings which organizations should follow sequentially. First level of training involved discussion of security threats and organizational sanctions. Training according to individual differences would be second level. Level three included training that considered combined effects of personality factors with perception of threat and sanction. Users can get training according to their personality profile which will improve the effectiveness of the training.

Aloul (2012), highlighted the need of security awareness in schools, universities, government and private sector. By analysing previous security awareness studies in UAE, they recommended cyberlaw enforcement by the government. CERT can help in the establishment of law and awareness campaigns among public. Organizations should initiate awareness among employees using posters, emails, newsletters. Educational institutes should include security topics in curriculum. These educational campaigns context should be comprehensive enough to increase knowledge leading to changes in behaviour. Arachchilage and Love (2014), analysed student's awareness and attitude towards phishing threats. They concluded that both conceptual and procedural knowledge positively impact self-efficacy which could enhance user threat avoidance behaviour, as it was known that self-efficacy had strong correlation with knowledge. Security education approaches should consider a combination of conceptual and procedural knowledge for better effects on security behaviour. Security awareness can also enhance students' self-efficacy to detect deception in a scareware message and changes perception of source trustworthiness as evident in a study by Ormond *et.al.*, 2016.

Security knowledge as a result of awareness or training program will improve protection behaviour among users (Srisawang *et.al.*, 2015). Security awareness significantly impact security practices of next generation technology users – students. Security trainings increase awareness level, so educational institutes should conduct awareness events regularly. By making information security part of their curriculum, awareness towards security practices can be improved among students (Muhirwe and White, 2016; Stanciu and Tinca, 2016). The awareness programs designed for students should be comprehensive (Al-Janabi and Al-Shourbaji, 2016; Kim, 2014), continual (Warkentin *et.al.*, 2016), persuasive (Johnston and Warkentin, 2012). While its content should be changed continuously to catch attention (van Schaik et.al., 2017). It should be designed according to their cultural orientation (Arpaci and Baloğlu, 2016; Farooq *et.al.*, 2015; Kruger *et.al.*, 2011), and conveyed by competent and credible source (Johnston and Warkentin, 2012).

2.2 Security Awareness Frameworks in Educational Institutes

With the increased use of information and communication technology (ICT) in educational institutes, the importance of security awareness among youngsters needs to improve. Walaza *et. al.*, 2015 addressed it by integrating the ICT security awareness into South African education system in the form of framework - ICT Security Awareness Framework for Education (ISAFE).

They took the building blocks of framework from different models and frameworks of ICT security and ICT in education. They added six new building blocks to fill the gap between ICT in education and ICT security. They proposed to have security initiatives in South African official language, ICT security awareness in Curriculum, ICT security office to enhance ICT security awareness among learners, ICT security information repositories in all public areas. All these initiatives made the framework relevant to South Africa context to boost their security knowledge and behaviour.

Kortjan and Von Solms, 2014 also proposed a cyber-security awareness framework after performing comparative analysis of four developed countries. They analysed the national cyber security awareness and educational strategies of USA, UK, Australia and Canada to identify the key factors. A five-layered framework included all the government, private and academia sectors as responsible units and partners. They have targeted all the audience educators, learners, parents and guardians according to their roles. Topics, contents, medium and tools were also part of framework. Progress was monitored by periodic reports and success indicators. Framework was layered in the context of Plan-Do-Check-Act (PDCA) cycle and verified by using four elite interviews. This framework can help South Africa to define national cyber security awareness campaign.

Ramalingam *et.al.*, 2016 proposed a model for the assessment of security awareness with six elements: effective usage, organization awareness, threats awareness, protection awareness, content awareness and security practice. They assessed ISA level of higher education members' students, academic and technical staff from 17 educational institutes. Using proposed security awareness model, they identified the awareness level, familiarity with policies and security practices followed by the users. Their results indicated that ISA at individual level was considerably better than institutional level, which could be improved by policy, security standard compliance, reporting and awareness programs. They emphasized not only the implementation of organization specific awareness program but also emphasized accountability of the entities in educational institutes by confirming policy compliance. In another study, Marks and Rezgui, 2009, proposed an IS security awareness sequential model to promote ISA by using design theorizing concepts and establishment of IS security policy, campaigning and advertising, training, reward and punishment, evaluation and readjustment. They suggested the combined use of multiple ISA approaches – training, campaigning, reward and punishment. Their combined effect increased the effectiveness of the ISA and influenced user behaviour toward security compliance.

Awareness programs bring changes at individual, organizational and technological levels, as these changes are interrelated. Awareness programs change individual perception, attitude, behaviour, habits and organizational cultures (Da Veiga and Martins, 2015). Tsohou *et.al.*, (2015) proposed a framework comprised of Actor-Network Theory, Structuration Theory and Contextualism, which was used to analyse and manage changes that occured at individual, technological and organizational level by security awareness programs. Actor network theory

used to study the social elements effect on technology, while structuration theory to explore the changes of human interaction on the organizational structures,and contexutualism to see the relationship between content, context and process of change. This framework highlighted the interrelated changes occur at individual, technological and organizational level by analysing the changes in information security awareness.

Vance *et.al.*, (2014) used a new technique and new direction to IS research. They measured risk perception using electroencephalography (EEG) via event-related potentials (ERPs), which in turn measured neural responses triggered by specific actions. Iowa Gambling Task (IGT), a technique from Neuroscience and Psychology field was used to measure neural responses to positive and negative feedback to predict users' information security behaviour. This study took the sample of university students and compared the result of EEG measures with self-reported measures and concluded that EEG measures can predict security behaviour whether information security is salient or not. Whereas self-reported measures are ineffective or effective to predict security behaviour when Information Security are not salient and salient respectively. This study evident that emotions such as fear and uncertainty are difficult to measure through self-reported measures. As through self-reported measures participants cannot reflect their actual attitude towards information security. However, participants can respond consciously after an incident in case of information security incidents became salient. So, author suggested the use of NueroIS methods such as EEG, fMRI to predict information security behaviour without measurement biases. Fear appeals also impact user intention to comply with security practices as defined by Johnston and Warkentin, 2010. They took faculty, staff and students in a laboratory experiment to study the influence of fear appeals on the compliance of end user. They observed the impact of fear appeals with other factors like self-efficacy, response efficacy, threat severity and social influence.

2.3 Factors Influencing ISA

In today's competitive era, organizations of different forms and different sizes need to have a security management plan. All the stakeholders of an organization must be conscious about information security. Role of every individual is required for the successful implementation of security solutions. The importance of Information Security Education (ISE), Information Security Training (IST) and Information Security Awareness (ISA) cannot be overlooked by any organization (Amankwa *et.al.*, 2014). NIST SP 800-50 defines Education, Training and Awareness according to their goals and targets users in the form of a learning continuum. Awareness addresses all the users and focus their attention towards security and behavioural change respectively. Training addresses the IT users and provides knowledge about security basics to produce skills and competencies. While education targets security specialists and professionals to refine their skills according to their roles and responsibilities. Education, Training and Awareness addresses "why", "how" and "what" of information security according to their goals (Muhirwe and White, 2016). Amankwa *et.al.*, 2014 defined ISE, IST and ISA in the form of focus, purpose and method attributes. ISE developes understanding using seminars,

discussions as delivery method of developing skills to ensure Confidentiality, Integrity and Availability (CIA) of an organization. IST focuses on security knowledge specific to their roles through workshops and seminars. ISA directs attention towards protection of information through posters, videos and other electronic media. Users whether they get Information security education, training and awareness, it influences the security behaviour of the recipients.

Information security awareness is affected by multiple factors which can be categorized as individual factors, organizational factors, environmental and cultural factors. Various studies showed relationship of these factors with information security awareness and its influence on information security behaviour. In most studies ISA assessment was applied at organizational level (Chan and Mubarak 2012; Stanciu and Tinca, 2016), whereas some studies assessed ISA at individual level (Ismailova and Muhametjanova 2016; McCormac *et.al.,* 2017). These studies showed varying results according to the environment where it applied. Factors highlighted in different studies are summarized in Table 1.

2.3.1 Individual Factors

Information and communication technologies are accessible to every individual, making everyone a part of global community. It surrounds an individual with advantages as well as risks. Individual factors differentiating an individual from other include age, gender, personality, behaviour, attitude, knowledge (McCormac *et.al.,* 2017). Variability of these factors can impact user's security awareness. Students between 18 – 30 age seem to be at most risk because of the increased use of internet, they are even higher victims of phishing email than elders (Öğütçü *et.al.,* 2016; McCormac *et.al.,* 2017). Studies showed significant positive relationship between age and information security behaviour, indicating olders have better behaviour toward information security (McCormac *et.al.,* 2017). With the growing age, individuals get more knowledge and better ISA level. Male students were found to have better knowledge and ISA level than female students (Farooq *et.al.,* 2015). In a study by Hamid and Zeki, 2014, found no difference between male and female participants regarding security issues awareness. Vance *et.al.,* 2012 didn't find gender differences regarding policy compliance. Halvei et.al., 2016 found gender as insignificant in affecting security behavior of participants. McCormac *et.al.,* 2017 highlighted the requirement of more research regarding age differences in security behaviour. Despite the large number of news about cybercrimes, the cybercrime knowledge is quite low and students are mostly not aware of many aspects of cybercrime. (Ismailova and Muhametjanova, 2016).

Individual behaviour towards technology usage is important to assess as it has a direct effect on information security (Öğütçü *et.al.,* 2016). Kruger and Kearney, (2006) developed a model for measuring security awareness by defining it in three dimensions of Knowledge, attitude and behavior. According to this definition ISA emphasizes on increasing knowledge in a way that influences attitude which will eventually change behaviour towards information security. McCormac *et.al.,* (2017) and Pattinson *et.al.,* (2015)also used in their study Kruger definition of

ISA. The definition of ISA in terms of knowledge, attitude and behavior aligns with the KAB model (Parsons *et.al.,* 2014; Parsons *et.al.,* 2017, McCormac *et.al.,* 2017). Originating from the field of psychology, Knowledge-Attitude-Behaviour (KAB) model, is used to assess ISA in terms of knowledge of policies, procedures, and understanding of why to use these policies and procedures (attitude), and what they actually do (behaviour) (McCormac *et.al.,* 2017).

Ögütçü *et.al.,* 2016 proposed four independent scales to assess individual's behaviour and awareness toward information technology. Risky Behaviour Scale (RBS), Conservative Behaviour Scale (CBS), Exposure to Offence Scale (EOS) and Risk Perception Scale (RPS) were proposed with respect to internet usage. It showed significant differences among three samples groups; students, academic and administrative staff. Students were exposed to crime at greater rate, as their ratio of risky technology usage is higher making them more vulnerable. Increased exposure to risks increases their threat perception as well. Administrative staff generally have the lowest risk perception and education level seems to affects awareness of information security. Habits believe to have an important role in employee compliance along with information security policy. Vance *et.al.,* 2012 observed habits in the form of past and automatic behaviour and its influence on components of Protection Motivation Theory (PMT). Components of PMT vulnerability, perceived severity, reward of threat appraisal and response efficacy, self-efficacy, response cost of coping appraisal have significant impact on employees' intention to comply with security policies.

Organizations having policies and security controls like firewall in place but still face challenges. Employees with intention to comply still engage in risky behaviour reflecting non-malicious risky behaviours. To measure actual user behaviour not only behavioural intention but other factors of personality also shows variance in behaviour (Shropshire *et.al.,* 2015). Personality traits have been used to predict various behavioural outcomes. The most commonly used Big five personality model consist of 5 factors: neuroticism, extraversion, openness, agreeableness and conscientiousness. Individuals with different personality react differently to same situation. So, these factors are important in evaluating ones' response (McBride *et.al.,* 2012). Shropshire *et.al.,* 2015 investigated the information security behaviour by the adoption of a web-based security software. They incorporated conscientiousness, agreeableness of personality and perceived ease of use, perceived usefulness of attitude and behavioural intent and its positive influence on behavioural adoption. Conscientiousness and agreeableness were observed as two most influencing personality factors in an organization. McCormac *et.al.,* (2017), analysed personality traits and risk taking propensity factors. The individuals with more conscientiousness, agreeableness, openness and less risk-taking propensity have higher levels of ISA. Pattinson *et.al.,* 2015 study showed that users' accidental naïve behaviour was less risky if they were more open and conscientious while less impulsive, older and have less familiarity with computers.

Continuous standard or policy compliance is difficult to maintain as compared to initial adoption. Organizations react more actively to the news of active attack affecting other organizations like

"WannaCry". But with the passage of time as the news fade away, organizations perceive as their chances of being the victim don't exist. For motivating individual toward continuous protective behaviour after initial use, Warkentin *et.al.,* 2016 used the constructs like perceived threat severity, perceived threat susceptibility, self-efficacy as antecedents of behavioural intent were significant determinant of continuance behaviour. Perceived extraneous circumstances – events which are unplanned and affect behaviour – are also direct determinant of continuance behaviour. As continuance behaviour, will help organizations to have better policy compliance. Hu et.al., 2012 also found a significant positive impact of personality facet, dutifulness on intention to comply. Their results strongly indicated that personality could play a significant role in shaping the compliance behavior.

2.3.2 Environmental Factors

Environmental factors like individual factors play an important role in influencing security behaviour. Factors including area of living, peer performance, social pressure were considered by different studies. Study by Farooq *et.al.,* 2015 showed that students from rural areas had less score for knowledge and behaviour toward ISA as compared to urban students. Behaviour of international students toward information security found better than local students.

Insider attack rate is increasing even in the organizations with policy in place. Persuasive communication was used as a mean to modify intention, attitude and behaviour effectively (Fishbein and Ajzen ,1975). Persuasive messages with element of threat, known as fear appeal also used in organizational communication. Fear appeals were used as influential tool for practicing protective behaviour with impact on intention to comply (Johnston and Warkentin, 2010). Fear appeals influence seemed helpful in initial compliance but it evaded with the passage of time (Warkentin *et.al.,* 2016). As users perceived less danger of threat and found security practices as time consuming activities, so their compliance level decreased ultimately affecting the organizations (Puhakainen and Ahonen 2006).

Warkentin *et.al.,* 2016 developed a model, to solve the individual continual engagement problem in securing organization information. This model was used to solve the acceptance discontinuance anomaly with constructs of PMT named as perceived threat susceptibility, perceived threat severity and self-efficacy. They found the model, useful for security administrators to align user behaviour with organizational security behaviour, after performing the study on undergraduate students of two universities.

Ahlan *et.al.,* 2015 have taken the peer performance and social pressure as environmental antecedent. They have seen that peers and family members have influence on user's intention toward security behaviour. Interaction between peers increases knowledge transfer which could be helpful in maintaining collaborative secure environment. Social environment influences one's opinions, beliefs, judgments and practices. Result showed self-attitude, policy compliance, training program and peer performance had positive influence on individual ISA. Religious

indicator and training program also showed significant relationship with ISA of higher education.

Srisawang *et.al.*, (2015) observed environmental influence by considering personality factors: conscientiousness, prior experience, perceived value of data and environmental factors like subjective norm, security knowledge and safeguard cost as potential benefit of security measure. Subjective norm as perceived social pressure showed influence on user willingness towards protective behaviour with positive effect on coping appraisal. It also increased user's ability of threat identification and associated dangers leading to positive influence on threat appraisal. Threat and coping appraisal had positive impact on protective behaviour. Results showed security knowledge as environmental factor had strongest effect on coping appraisal which subsequently influenced protection behaviour. Knowledge of threat was not considered enough if one did not know how to avoid them and at the same time knowledge of security measures was not helpful if one did not recognize threats. Hanus and Wu, 2016 used the protection motivation theory (PMT) constructed threat and coping appraisal as threat awareness and countermeasure awareness. They introduced awareness as a predictor of threat and coping appraisal. Perceived severity, response efficacy, self-efficacy showed strong influence on security behaviour. This multidimension awareness showed that only threat and fear was not enough, user should be motivated and confident of protection measures.

Haeussinger, 2013 studied peer behaviour and secondary source influence as environmental variables. They found that Information Security Policy-compliant behaviour influenced peer behaviour toward security practices. Information circulated through secondary sources like newspaper, internet, TV could be helpful for engaging large recipients. These external sources increased individual understanding of security threats and had an impact on awareness toward information security. Results showed positive impact of secondary source information on individual ISA (Srisawang *et.al.*, 2015). According to Johnston and Warkentin, 2012, influence of source credibility on user behaviour and attitude had a strong positive impact on recommended actions compliance. Influential leaders should be competitive, trustworthy with good reputation leading to better IT acceptance.

2.3.3 Cultural Factors

Users being the weakest link in the security loop are susceptible to lack of awareness by involving in unsafe browsing, downloading suspicious material, sharing password among family and peers and using unprotected home wireless networks. The technology shift with virtual organizations brings the official tasks into unprotected home environment providing more opportunities to attackers (Arachchilage and Love, 2013). With all these changes, cultural factors also play their part in influencing individual behaviour toward security. Culture include norms, values and belief that influence an individual attitude and behaviour (Arpaci and Baloğlu, 2016). Culture is a group – level phenomena but individual differences exist within cultures which highlight the need to assess culture at individual level. Each individual is influenced by different

cultures like national and organizational cultures (Straub *et.al.*, 2002). Since organizations are becoming global and multicultural requiring models and methods validity to be tested across different cultural settings. This issue is highlighted by Karjalainen *et.al.*, 2013, by explaining effectiveness of different approaches in multicultural environment for changing employees' information security behaviour. They assessed IS behaviour of employees from Finland, Switzerland, UAE and China to see the effectiveness of different learning paradigm in different cultures on security behaviour. They found different cultural – dependent reasons that explain employees' IS behaviour and different learning paradigm adoption in different countries. Behaviourist learning methods, Authority, Imitation and observation, Punishment reward and monitoring, Cognitivist learning methods, Constructivist and social constructivist learning methods were used as cultural-dependent reasons. They found that China prefers behaviourist learning methods while constructive and social constructive learning methods were preferable in Switzerland. Punishment and reward were considered effective in China and UAE while Switzerland found employees monitoring and sanction inappropriate. Cultural – independent reasons which explain employee IS behaviour across cultures were work experience, morals and upbringing, work environment, professional identity, media, social conformity and active communication. They suggested customized security interventions, security policies and procedures according to cultural and local needs.

Based on Hofstede, 2001 cultural dimensions were Power distance, Individualism versus collectivism, Masculinity versus femininity, Uncertainty avoidance, Pragmatism, and Indulgence. Flores *et.al.*, 2015 studied the intention-action relationship regarding external threats of social engineering among employees of two different national cultures. They examined relationship between employee's intention to resist social engineering and their self-reported behaviour as well as observed actions with moderating effect of national culture. Their results showed cultural influence on relationship between employees' intentions and behaviour. U.S and Swedish employee showed differences in reported behaviour and behaviour in practice. US culture showed strong prediction of actual behaviour through scenario-based surveys. They haven't considered the organizational differences studied by Kruger et.al., 2011. Kruger *et.al.*, 2011 conducted a study between two different universities and found the effect of cultural factors on security awareness of students. Their mother tongue (language) and area where they completed their secondary education had influence on their security awareness, which they needed to be considered while developing awareness programs.

Hu et.al., 2012 studied the role of top management and organizational culture influence on security compliance behavior of employees. They highlighted the two aspects of organizational culture how culture shape employee value, cognition and behavior among members and influence of organizational leadership on organizational culture. Authors pointed out that top management and organizational culture complement each other in shaping employee behavior intentions and therefore behavior towards compliance. This study used the CVF organizational culture model used by van Muijen et.al., 1999 originally of Quinn, 1988 other than Hofstede

cultural framework. Out of four they focused on two cultural dimensions from the CVF model: goal orientation and rule orientation. The study implicated that rule and goal oriented culture have significant influence on employees' cognitive beliefs about information security. The results also suggest that top management is the most important external factor that shapes employee behavior towards information security policy compliance and shapes organizational cultural values.

Arpaci and Baloğlu, (2016) studied the impact of cultural collectivism on knowledge sharing among IT undergraduates. Collectivist and individualist cultural dimension considered as main reason for cultural differences in a society. Individualism and collectivism have positive impact on students' attitude and subjective norms about knowledge sharing. Students with collectivistic culture were more open to share knowledge with peers. Students cultural dimensions should be considered while designing any educational or awareness activity regarding information technology. Collaborative learning environment facilitated students regarding learning through cooperation with peers. Educational institutes can create virtual collaborative environment by creating blogs, social groups while instructors can play the role of a facilitator. These knowledge sharing facilities can improve student awareness and behaviour as culture has influential effect on user behaviour. In another study, Flores *et.al.,* 2014 investigated the impact of behavioural information security governing factors on sharing of security knowledge in an organization. Their observations concluded that national culture having significant effect on knowledge sharing and decision making. Vance *et.al.,* 2012 suggested to change organizational culture and working environment to encourage information security policy compliance. Few studies addressing information security awareness with cultural dimensions in education sector were found, however more research needed to be done in respective domain.

Summary:

Using systematic review analysis, the studies about information security awareness in educational institutes were investigated. Through analysis, the factors that have influence on user behaviour towards information security were observed. Effects of individual, environmental and cultural factors on students, academic and administrative staff were examined as well. Security behaviours observed to be affected by the individual, organizational and environmental factors so only those training and awareness programs proved as more effective which were designed according to the environment of the participants. To get benefits at its best, these programs should be developed according to the target audience with preferable environment and cultural norms in consideration. These awareness campaigns are not just get and forget activities, these requires continuous emphasis and workup to keep its benefits active. To achieve higher level of information security, a comprehensive information security program is required which could target actual behavior by understanding different factors like organizational, cultural and individual (Hu et.al., 2012).

CHAPTER 3

Research Methodology

This chapter presents the detailed overview of the research approach that was assumed in thesis work. Different research methods and methodologies were explored and hybrid research methodology was selected. The different phases of research are comprehensively explained in this chapter. All the selected research methods have been followed at different stages of our research process, as each of the method is appropriate for different research scenarios under consideration.

3.1 Introduction

Research is a logical and systematic process of searching for new and unknown facts and gain information to advance state of the art. It is an investigation which leads to discovery of hidden truths which eventually make progress in the field. Research methodology is the systematic and theoretical analysis of the methods to solve the research problem. It is a science of studying how research is to be carried out scientifically. In research methodology, researcher studies the methods used to investigate the research problem with the underlying logic to select the applicable techniques for the research problem (Kothari, 2004). Main objectives for the presented thesis include:

- Get in-depth knowledge in the domain of information security awareness.
- Get insight into the challenges of influencing security behavior through ISA programs.
- Develop hypothesis through literature survey and analysis.
- Validate the formulated hypothesis through evaluation strategies.
- Design the tailored awareness program framework as per statistical analysis outcomes.

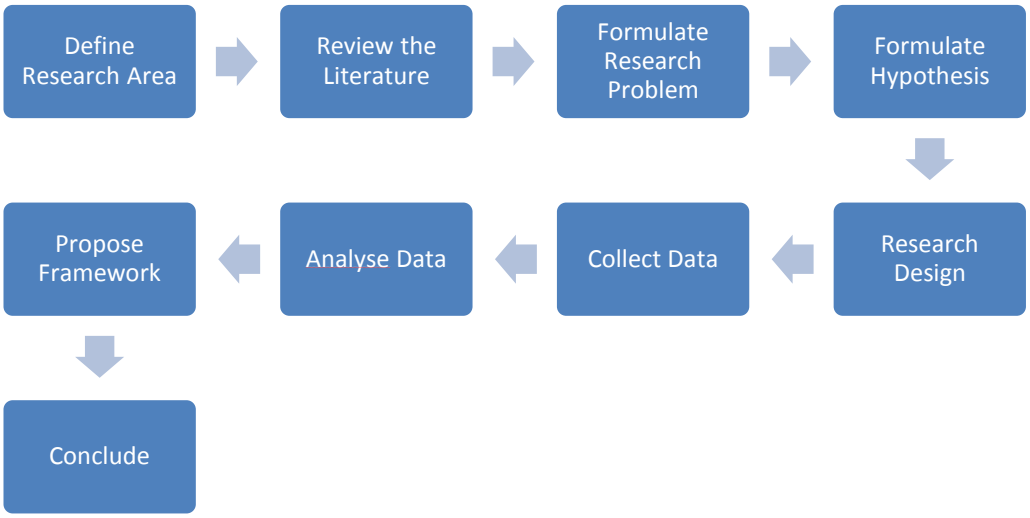


Figure 3.1 Research Methodology

3.2 Thesis Research Approach

To carry out the research work, Hybrid research methodology has been used to accomplish the diverse thesis aims and objectives. In this research we aim to address the environmental, cultural and behavioral factors effect on information security awareness. Therefore, descriptive, conceptual, empirical and deductive research methodologies have been combined. The brief description of all the steps followed in the research process is given as shown in Figure 3.1.

3.2.1 Define a research area

In the first step of research process, Information security awareness was selected as per general domain of study. Through deductive research approach, in-depth survey on the proposed information security awareness programs has been conducted. On the basis of the facts and observations derived out of this literature survey, we have formulated our research problem statement and hypothesis.

Our research thesis emphasize on the security awareness techniques and frameworks which should not only focus knowledge but bring change in behavior of individuals according to their personality. Individual factors like personality traits, environmental and cultural factors collective impact on security awareness was targeted for the current study. Deficiencies in security awareness frameworks to effect behavior were evident through literature. So, our study will fill this gap by making improvements in ISA framework for targeting behavior.

3.2.2 Literature Survey

The second phase was to conduct extensive survey on ISA and associated factors from behavioral, social and physiological theories. The literature demonstrated that there are a number

of internal and external factors that motivate an individual towards security behavior which leads us to following questions:

1. Explore the determinants of individual security behavior.
2. What theoretical and practical implications are suggested by researchers for improving ISA?
3. What methods and frameworks are used by researchers for improving ISA in terms of Knowledge, Attitude and Behavior?

We have carried out the literature survey using two main types of research approaches namely the conceptual and empirical research approach. We have conducted the conceptual survey to explore the concept and theories used in information security awareness. During this survey, we perform comprehensive study of theories and various assessment techniques which are proposed to investigate the security awareness level of participants. After detailed conceptual survey, we conducted empirical survey to explore the techniques and frameworks proposed to improve the effectiveness of ISA programs. This review helps us to further explore the techniques to improve the behavioral outcomes of ISA programs. The comprehensive literature review of existing techniques and methods in ISA leads us to formulation of our research problem.

3.2.3 Formulate Research Problem

Our extensive literature survey conducted in previous phase of survey lead us to formulate research problem.

1. There is a need to analyze the combined effect of environmental, cultural and individual factors including personality traits on ISA.
2. There is a need to identify deficiencies in the frameworks of security awareness programs that became obstacles to achieve the goals of ISA programs.
3. There is a need to improve the ISA framework with strategies and techniques for influencing individual behavior as per his/her personality, environment and cultural effects. This leads us to get the improved behavioral outcomes of ISA programs.

3.2.4 Develop Hypothesis:

Deductive research method has been used to develop the hypothesis for our research on basis of state-of-the-art literature survey and the problem statements formulized in the previous step. Our hypotheses are divided according to different constructs used in this study.

i) Do personality traits of an individual have influence on the ISA level in terms of knowledge, attitude and behavior?
ii) Does the environmental factors; secondary source influence and peer pressure have any relation with ISA of an individual?
iii) Does the rule following culture of an organization positively influence an individual's ISA level?

iv) Does individual differs in terms of knowledge, attitude and behavior due to technical and non-technical background?

3.2.5 Research Design

The research design has been formulated by using the analytical research approach which includes the analysis of existing research models for the assessment of ISA and propose assessment model for solving the identified problems. The research design has been divided into two sub-phases which includes the designing of material instrument and the selection of subject targeted. The assessment method was a paper-based questionnaire divided into five sections with 55 questions:

i) Personality traits
ii) ISA as knowledge, attitude and behavior according to 4 focus areas like password management, internet use, email use, social media use
iii) Secondary source influence on ISA
iv) Rule following influence on ISA
v) Peer pressure positive/negative influence on ISA

The research model was formed using the aforementioned constructs categorized as Individual, environmental and cultural factors. This model assessed students' knowledge, attitude and behavior towards information security awareness through these constructs.

3.2.5.1 Material Instrument:

Quantitative research design has been used to investigate the ISA level of students. Through quantitative research, numerical description of the phenomenon has been created by coding verbal or textual data. Questionnaire assessment method has been selected to collect data for the current study. The scale was developed using ISA as dependent and personality traits, secondary source influence, peer pressure and rule following as independent variables and a set of demographic questions. The dependent variable ISA composed of three equivalent dimensions named as knowledge (what does a person know); attitude (how do they feel about the topic) and behavior (what do they do). Each one of these dimensions, subdivided into six focus areas by Kruger and Kearney, 2006. In our study we considered only four focus areas according to the organization and participants under consideration. The focus areas selected for the current study includes: password management, email use, internet use, social media use. Each focus area is further divided into subareas and we included selective subareas according to our case study, resulting in total 11 areas of interest as shown in figure 3.2. Through these focus areas; we will be able to understand different aspects of ISA relevant to multiple areas of interest (Parsons *et.al.*, 2017).

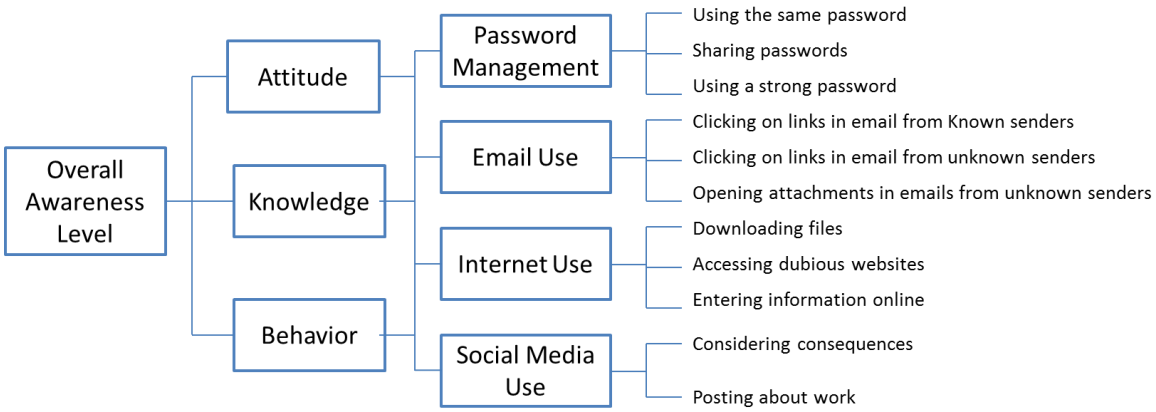


Figure 3.2 Focus areas and sub areas of HAIS-Q

To measure the ISA in terms of knowledge, attitude and behavior, we used the Human Aspect of Information Security Questionnaire (HAIS-Q). HAIS-Q is developed and validated by Parsons *et.al.*, (2014). HAIS-Q is validated by Parsons *et.al.*, (2017) by two case studies on 112 university students and 505 working Australians. Both the case studies showed HAIS-Q predictability of information security behavior which designated it as a robust measure of ISA. HAIS-Q is based on the supposition that with increasing users knowledge of information security policy and procedures, their attitude improves, which ought to reflect improved behavior towards information security (Parsons *et.al.*, 2014; McCormac *et.al.*, 2017). The description of knowledge, attitude and behavior as specified in HAIS-Q by Parsons is related to Knowledge-Attitude-Behavior (KAB) model. The definition of ISA in terms of knowledge, attitude and behavior aligns with the KAB model (Parsons *et.al.*, 2014; Parsons *et.al.*, 2017, McCormac *et.al.*, 2017). To measure the dependent variable ISA, we selected the 33 statements from HAIS-Q, on a five-point Likert scale. The scale ranged from 1 as 'Strongly Disagree' to 5 as 'Strongly Agree'.

To investigate the potential impact of individual, environmental and cultural factors on knowledge, attitude and behavior, we considered these factors as dependent variables. The selection of independent variables is according to the aim of research and requirements of the organization being examined. In line with McCormac et.al., (2017), who indicated that personality characteristics were associated with high scores of ISA. So these personality factors are important to understand an individual ISA. The Big Five personality model often referred to as The Big Five, is extensively used to describe different aspects of personality (Shropshire *et al.*, 2006). It comprises of five aspects: agreeableness, neuroticism, openness, extraversion, and conscientiousness (Costa & McCrae, 1992; John & Srivastava, 1999).The BFI of 15 items (Hahn *et.al.*, 2012) which measures personality of an individual according to Big Five magnitudes of inventory. Traits measured through Items are rated on a five point Likert scale (ranging from 1 as 'Strongly Disagree' to 5 as 'Strongly Agree').

Peer pressure and secondary source influence (SSI) were included to measure the influence of peers and information from different sources on one's security behavior. Both of these variables are categorized in environmental construct to measure environment effect on one's behavior. Social environment can influences the practices, opinion, belief and actions of individuals which was affected by opinion of other peoples (Hui et.al., 2009). Several studies in the information security domain suggest that individuals' understanding of security threats and their security behavior are positively related to information received from mass media including newspapers, radio, internet, and TV (Herath and Rao, 2009b, Siponen et.al., 2009, NG and Rahim 2005). The secondary source influence item is selected from (Brown and Venkatesh 2005) on five-point Likert scale from 1 as 'Strongly Disagree' to 5 as 'Strongly Agree'. We developed the peer pressure items according to our survey requirements to measure the peer pressure influence on students' security behavior. Peer pressure construct consist of 3 items on five-point Likert scale from 1 as 'Never' to 5 as 'Always'.

As Tsohou et.al., (2015) emphasized the individual and cultural factors importance in creating ISA programs, we selected cultural factors to get in-depth understanding of ISA. Rule following was included in survey as an instrument to measure organization culture effect on students' security behavior. As in our sample we have students from both the military and civilian institutes. We measured the rule following culture effect on students' attitude and behavior towards security. These items measured student's attitude towards rules and their tendency towards following organizational rules related to information security. We developed the rule following items according to existing rules of the target organization. The three items were developed on five-point Likert scale ranging from 1 as 'Never' and 5 as 'Always'.

The survey also consisted of general demographic data as control variable in the first section, including age, gender, institute, degree, discipline and semester. The demographic information was used exclusively for the purpose of comparison and further analysis of data. The participants were assured that their privacy was of supreme concern. Their participation would not be connected to them individually, and their identity would remain anonymous and not disclosed throughout the analysis.

3.2.5.2 Sample & Population:

The sample was drawn from twin cities of Pakistan including Rawalpindi and Islamabad. This study included students from different institutes of National University of Science and Technology located in Rawalpindi and Islamabad, classifying them into technical and non-technical students. The research sample was a total of 501 students out of which 487 were true responses and 14 were excluded as outliers. From 10 different institutes of NUST, 297 technical and 190 non-technical students participated in the study as shown in Table 3.1. Out of 487, 288 were males and 199 were females. Approximately 17% of participants were aged between 18 or under range, 75% were in age range of 19 – 24. This left approximately 6% in the 25 – 31 age category, and 2% aged 32 – 38 and 39 or above ranges.

Among the participants, 439 students were from Bachelors and 45 from Master's Program and 2 of them were PhD students. As security awareness is everyone's responsibility, so we selected both the technical and non-technical students to analyze the security knowledge influence on their behaviors toward technology use in daily activities. Everyone should be concerned about information security as technology is integral part of todays' Millennials. It is not bound to the one who is in information technology field. The survey focused on investigating the influential factors that affect knowledge, attitude and behavior of an individual towards information security. And examine the knowledge influence on their security behavior whether they are from technical and non-technical field.

Total Sample (501)	Considered	487
	Discarded	14
Students	Technical	297
	Non-Technical	190
Gender	Male	288
	Female	199
Degree	Bachelors	439
	Masters	45
	PhD	2
Age	18 or Under	81
	19 – 24	366
	25 - 31	33
	32 - 38	3
	39 or Above	3

Table 3.1 Demographic data of respondents

3.2.6 Collect Data:

The quantitative approach used in this study to assess the ISA level of students in the form of Knowledge, attitude and behavior and to investigate the combined effect of individual, environmental and cultural factors on ISA. Primary data was collected on a paper based questionnaire over a period of 5 months from May 2017 to September 2017. As explained previously in Table 3.1, 501 students were included in the sampling frame. The self-administrated survey was collected directly from the participants. The estimated time to fill the form was 10-15 minutes. The study utilized random probability sampling, permitting generalization of the results to larger populations. Creswell, 2009 found random sampling was a frequently used method in quantitative research as it provides generalizability. Therefore, the results were expected to represent the entire population.

Participation was voluntary, and the participant could quit the survey at any time. All responses did not retain any personal information about the participants beyond the demographic information provided. The two of the filled scanned questionnaires are included in Appendix B.

3.2.7 Analyze Data:

The data was analyzed using SPSS 22, including data coding and screening. After the data screening, outliers and responses with missing values were omitted from the sample using descriptive statistics. Out of 501 responses, 14 were omitted, leaving 487 true responses. Before doing further analysis, the reliability and internal consistency of the instrument was tested using Cronbach Alpha. Data was analyzed according to the theoretical model as shown in Figure 3.3. The indicator variables and constructs specifications were modeled in theoretical framework.

Construct interrelation was explored as structural model analysis. The structural model consists of individual, environmental and cultural constructs. Hypothesis testing was used for exploring the influence of one construct on another. Hypothesis was analyzed using coefficient of determination (R^2) and group difference testing. The result of these hypotheses is further explained in Chapter 4 Results and Analysis.

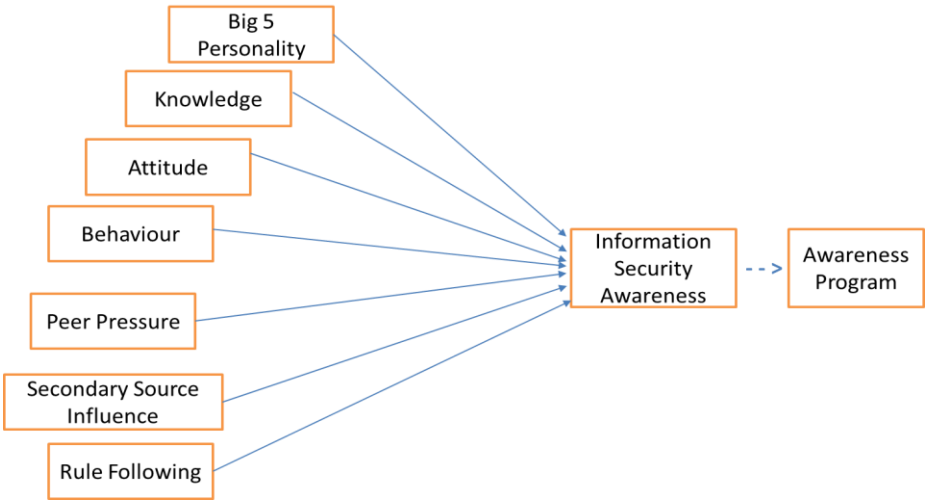


Figure 3.3 Theoretical Framework

3.2.8 Propose Framework

On the basis of results deducted from hypothesis testing, we improved the NIST framework (NIST SP 800-50) for ISA program. The framework is improved by selecting strategies and techniques which could address the deficiencies find in the analysis section. The strategies were selected to improve the behavioral outcomes of the framework on the basis of individual, cultural and environmental factors impact on individual ISA. We also proposed the ad-hoc model of ISA program for one of the institute of NUST.

3.2.9 Conclude

On the basis of the results calculated in the analysis section, interventions were defined in the last phase of the research. The deficiencies in NIST awareness program framework were mitigated by improving the framework on the basis of statistical analysis. These interventions will help in improving individuals' behavior towards information security awareness. An ad-hoc approach was used to develop an awareness program model for an institute of the target organization.

Summary:

This chapter has described the overall methodological approaches used for the current study and their significance. For the current thesis, hybrid research methodology is used which is a combination of descriptive, conceptual, empirical and deductive research methodologies. Using these different research methodologies, formulation of research problem, hypothesis development and ISA framework deficiencies were addressed.

CHAPTER 4

Results and Analysis

This chapter presents the results of our proposed work. The study was mainly focused on analyzing the relationship of individual, environmental and cultural factors with information security behavior. The survey measures how different factors affect student's level of ISA by collecting a set of factors from the literature and generating or selecting a number of related Likert items for each factor. The beginning of the chapter provides a description of the study's population, sample, and descriptive statistics. The next section contains a summary of the results of each hypothesis followed by detailed analysis of the results. The chapter concludes with a summation of the results and answers to the study's research hypothesis.

4.1 Reliability of Measurement Scale

Cronbach alpha is the most common measure of internal consistency ("reliability"). Reliability analysis is performed when we have multiple Likert questions that construct a scale and need to determine if the scale is reliable. The scale was developed to measure the information security awareness of students using KAB model emphasizing the focus areas like password management, internet use, email use and social media use. From the HAIS-Q questionnaire we selected the focus areas which are involved in students routine activities whether they are studying in a technical and non-technical discipline. Focus area of each category comprised of statements related to knowledge, attitude and behavior. The definition of ISA reflects KAB model which states that as the knowledge of information security policies and procedures increases, their attitude improves, which leads to improved information security behavior. In the current study, reliability analysis for knowledge, attitude and behavior were 0.470, 0.640 and 0.529, with a reliability level of 0.795 for the overall ISA.

The scale contains individual, environmental and cultural factors to investigate their effect on students ISA. For individual factors, we took demographics and Big Five model for analyzing personality traits of individuals and the underlying psychological mechanism which could have an impact on user awareness. Big Five model consist of the following five personality dimensions: extraversion, neuroticism, openness, conscientiousness and agreeableness. The current study found reliability analysis result with values 0.441 for conscientiousness, 0.668 for extraversion, 0.490 for agreeableness, 0.617 for openness and 0.706 for neuroticism.

The scale also included secondary source influence and peer pressure as environmental factors (Haeussinger, 2013). The environmental influence can be separated into primary sources and secondary sources. Primary sources include influence of peers such as family members, friends and co – workers (Brown & Venkatesh, 2005). Security behavior of co-workers has a certain impact on employees' ISA (Haeussinger, 2013). It is proven empirically that family members

and peers significantly affect an individual intention to behave responsible with respect to computer security (NG and Rahim, 2005). Secondary sources consists of information from mass media including newspaper, internet, TV. The positive impact of information from mass media about security threats on individual knowledge and behavior is assumingly large due to an increase in the recipients' level of ISA which is evident in a study by Haeussinger, 2013. The environmental factor peer pressure showed alpha level of 0.478 for the current study. The alpha level of factor secondary source influence cannot be calculated being a single item variable for the current study.

The cultural factor items were created according to the current study requirements. We take rule following as a cultural variable to examine the rule following culture among different institutes of NUST. For example MCS have students and teachers from military, the institute have a rule following and strict culture as compared to other institutes of NUST like SEECS, IGIS. The items were based on the rules which currently exist for internet and password use. The rule following variable showed alpha level of 0.381 for the current study.

4.2 Hypothesis:

4.2.1 ISA and Individual Differences:

$H1_a$: Openness personality factor have positive influence on Information security awareness.

Information security awareness was computed by aggregating the scores of an individual's knowledge, attitude and behavior. This computed score was used to inspect the relationship among dependent variables and ISA.

As shown in Table 4.1, correlation between individual personality factors and ISA showed significant positive relationship between agreeableness and ISA (r = 0.123, p < 0.001), Conscientiousness and ISA (r = 0.174, p < 0.001), Openness and ISA (r = 0.187, p < 0.001). Extraversion and neuroticism traits have non-significant relationship with ISA.

To further inspect the relationships between ISA and independent variables, a multiple linear regression was calculated to predict ISA based on personality traits, secondary source influence, rule following, peer pressure, age and gender. A significant regression equation was found F (12, 474) = 13.861, p < .000, with an R^2 of 0.260. As shown in Table 4.2 age and openness individual differences were the strong contributor. Which support the $H1_a$ hypothesis that openness personality trait have significant positive influence on ISA. The more openness to experience trait ones' personality have, the better their ISA level will be. Gender (β = - 0.043, p = 0.309) is not significant and age (β = 0.144, p = 0.002) has positive significant influence on ISA. This shows that student's awareness level increases with age. Based on these results we accept the $H1_a$ hypothesis that openness personality factor have positive influence on ISA.

Variables	Gender	Age	Degree	Knowledge	Attitude	Behavior	ISA	Extraversion	Agreeableness	Conscientious	Openness	Neuroticism	Secondary Source	Peer Pressure	Rule Following
Age	.004														
Degree	.066	.509**													
Knowledge	.006	.185**	.053												
Attitude	-.054	.093*	.055	.586**											
Behavior	-.021	.116*	.088	.515**	.569**										
ISA	-.029	.154**	.077	.827**	.873**	.817**									
Extraversion	-.028	.073	.020	.006	-.055	.024	-.013								
Agreeableness	-.065	-.033	-.012	.065	.113*	.132**	.123**	.123**							
Conscientious-ness	.034	.003	.039	.079	.151**	.209**	.174**	.091*	.148**						
Openness	.052	.015	-.034	.107*	.184**	.175**	.187**	.128**	.075	.230**					
Neuroticism	.272**	-.061	-.042	-.040	-.071	-.038	-.060	-.253**	-.162**	-.232**	-.159**				
Secondary Source	.055	-.027	-.014	.081	.272**	.242**	.240**	-.024	.136**	.178**	.145**	.015			
Peer Pressure	-.033	-.024	-.057	-.282**	-.293**	-.308**	-.350**	.072	-.171**	-.158**	-.009	.058	-.083		
Rule Following	-.146**	.009	-.126**	-.130**	-.205**	-.236**	-.227**	-.004	-.238**	-.126**	-.049	-.067	-.140**	.313**	
Mean				3.27	3.66	3.5	3.48	3.23	3.70	3.26	3.78	3.25	3.70	2.05	2.32
SD				0.46	0.53	0.45	0.40	0.87	0.70	0.67	0.69	0.93	0.96	0.79	0.84

*$p < 0.05$ (2 – tailed) ** $p < 0.01$ (2 – tailed)

Table 4.1 Correlations, means and standard deviations between knowledge, attitude, behavior, ISA, age, The Big Five personality factors, secondary source influence, peer pressure and rule following (*N* = 487)

Variable	B	T
Age	0.143	3.07**
Gender (Female = 2)	-0.042	-0.99
Agreeableness	0.001	0.03
Conscientiousness	0.064	1.49
Extraversion	-0.024	-0.58
Openness	0.131	3.14**
Neuroticism	0.01	0.22
Secondary Source Influence	0.173	0.42***
Peer pressure	-0.290	-6.81***
Rule Following	-0.128	-2.89**

*p < 0.05, **p < 0.001

Table 4.2 Summarized regression analysis of age, gender, agreeableness, extraversion, openness, conscientiousness, neuroticism, secondary source influence, peer pressure and rule following predicting ISA (*N* = 487).

$H1_b$: Conscientiousness personality factor have positive influence on Information security awareness.

Hypothesis $H1_b$ was rejected as results shows insignificant impact of conscientiousness (β=0.064, n.s)on ISA.

$H1_c$: Extraversion personality factor have positive influence on Information security awareness.

Hypothesis $H1_c$ was rejected as results shows insignificant impact of extraversion (β=-0.024, n.s)on ISA.

$H1_d$: Neuroticism personality factor have positive influence on Information security awareness.

Hypothesis $H1_d$ was rejected as results shows insignificant impact of neuroticism (β=0.01, n.s)on ISA.

$H1_e$: Agreeableness personality factor have positive influence on Information security awareness.

Hypothesis $H1_e$ was rejected as results shows insignificant impact of agreeableness (β=0.001, n.s)on ISA.

4.2.2 ISA and Environmental Factors

H2 : Information from secondary – sources have positive influence on students' ISA.

As shown in correlation table 4.1 secondary source influence is positively related to ISA (r = 0.240, p < 0.001). To test the hypothesis we further performed analysis through regression analysis in table 4.2. Which shows that secondary source influence (SSI) value is positive and highly significant (β = 0.42, p = 0.000). The analysis supports the H2 hypothesis that SSI has positive influence on students' ISA.

H3 : Peer – pressure negatively influences students' ISA.

Peer pressure as environmental variable has significant but negative correlation with ISA (r = -0.350, p < 0.001). Further analysis in regression table 4.2 shows that peer pressure has significant but negative influence on ISA. This means that the more peer pressure influence an organizational environment have, the less their ISA level will be.

4.2.3 ISA and Cultural Factor

Culture refers to beliefs, values and assumptions that a faction has learnt over time. Organization culture is set of procedures, practices and rules that employee follows in order to be successful in their environment (Schein, 1999). Organizational culture needs to be emphasized to reflect change in behavior towards information security. As effectiveness of information security control is dependent on the people who are implementing and using it. Likewise Information security culture within an organization emerges from the way in which people behave towards information security (Martin & Elofe, 2002).

Rule following was taken as cultural variable to analyze the different institute cultures within NUST. Through this cultural factor we will also analyze how is it influencing students' knowledge, attitude and behavior towards security awareness. As in our sample we have students from different institutes in which we have random sample of military and civilian institutes. Through this sample variation, we can investigate whether rule following culture in military institutes are influencing students towards behavioral change. And how much influence we can bring in security awareness of students through rule formation and enforcement.

H4 : Rule following positively influences students towards ISA.

In correlation table 4.1, rule following variable have significant but negative correlation with ISA (r = -0.227, p <0.001). For hypothesis testing, regression analysis shows that rule following has significant but negative influence on ISA (β = -0.128, p = 0.004). The more students directed towards rule the less their ISA is. So by rejecting the hypothesis we conclude that rule following does not influences students towards ISA. From this analysis we can deduce that rule formation does not help in influencing students towards security awareness. The summarized regression analysis is also shown in Fig 4.1.

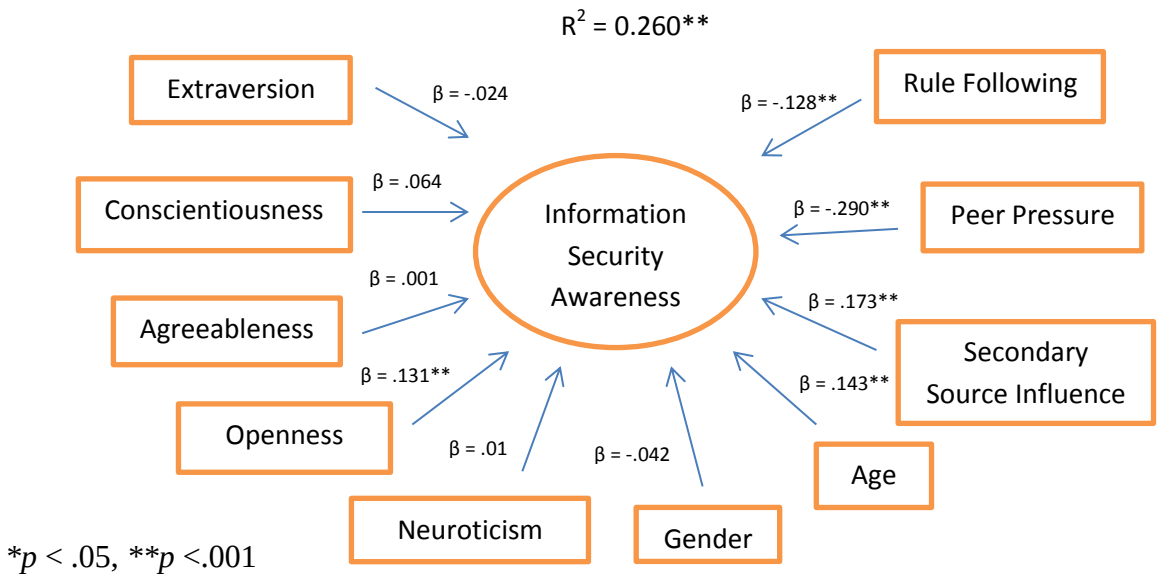


Figure 4.1 Variance described by the environmental, cultural and individual difference factors; openness, neuroticism, conscientiousness, agreeableness, extraversion, age, gender and secondary source influence, peer pressure and rule following.

4.2.4 Knowledge Difference among Technical and Non-technical students

H5 : There is a significant difference between security knowledge of technical and non-technical students.

For this hypothesis testing group of mean differences was calculated through – samples t-test. The two groups are technical and non-technical students. An independent – samples t-test was conducted to compare security knowledge in technical and non-technical students.

Before performing the t-test one have to meet 6 assumptions. In first assumption, we need to check that dependent variable should be measured on a continuous scale. In underlying study dependent variable is information security awareness (ISA) comprised of knowledge, attitude and behavior. All the three items are measured on continuous scale (measured from 1 to 5). Hence, meets the first assumption.

The second assumption is independent variable should be consisting of two categories. As in our study the students are categorized as technical and non-technical on the basis of discipline in which they are studying.

As third assumption independence needs to be tested. Independence is a procedural concern; it is assessed by examining the design of the study. In this assumption we ensure that no relationship exists between the groups and both groups have different participants. In our study both the technical and non-technical groups are independent and have different participants for each group.

Outliers are checked in fourth assumption of t-test. Outliers are data points within our data which do not follow the usual pattern. Outliers produce negative effect on the independent t-test, which reduces the result validity. By using boxplot graphs, we checked our data for significant outliers. We didn't find any extremes outliers in our data which fulfilled the fourth assumption.

In fifth step assumption of normality is tested. Shapiro – Wilks test was used to test the normality assumption. Which require hypothesis testing for interpreting the results. It worked by equating the null hypothesis as there is no significant difference from normality, and alternate hypothesis as there is significant difference from normality.

Tests of Normality

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Category	Statistic	df	Sig.	Statistic	df	Sig.
ISA	Technical	.030	297	.200*	.994	297	.334
	Non-Technical	.057	190	.200*	.992	190	.356

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Table 4.3 Normality Test of Technical and Non-technical groups

From the above table 4.3, $\alpha = .01$, given that $p = .334$ for the technical group and $p = .356$ for the non-technical group, we concluded that student categorized as technical and non-technical showed normal distribution for ISA. Therefore the normality assumption meets for the t-test. Normality results also evident from the histogram as shown below in Figure 4.2.

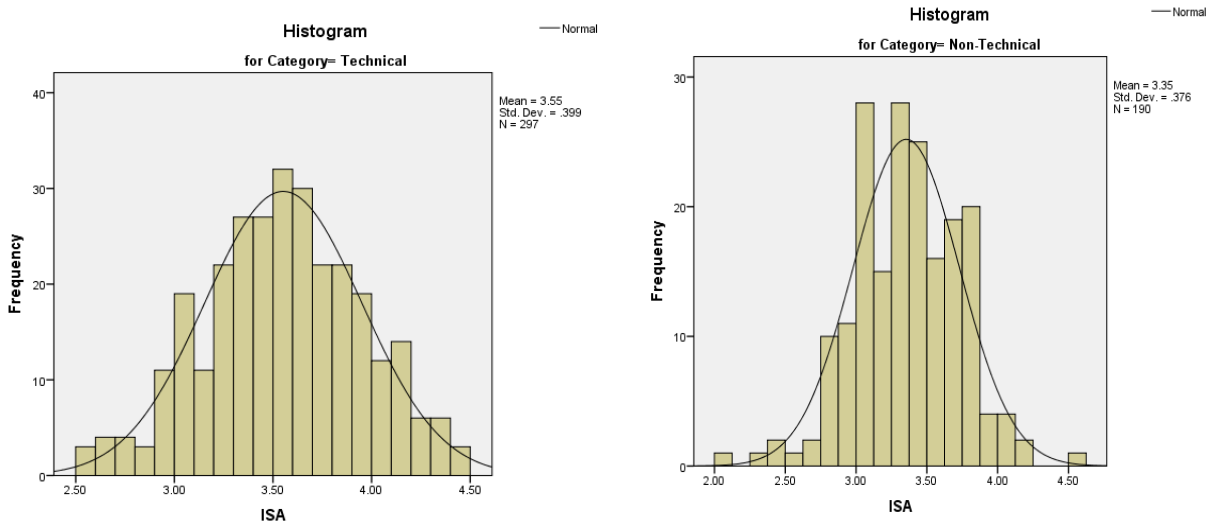


Figure 4.2 Histogram showing Normality results of Technical and Non-Technical groups

The sixth and last assumption is testing the homogeneity of variances. The Levene's *F* Test is the most frequently used statistic to check the assumption of homogeneity of variances.

		Levene's Test for Equality of Variances	
		F	Sig.
ISA	Equal variances assumed	.862	.354
	Equal variances not assumed		

Table 4.4 Levene's Test for homogenity of variances for H5

The *F* value for Levene's test as shown in Table 4.4 is 0.862 with a Sig. value of 0.354 is greater than alpha value ($p > 0.05$). So we accept the assumption of homogeneity of variances for further analysis.

After testing all the assumptions of t-test we performed the independent t-test for H5. Using an alpha level of .05, an independent – samples t-test was conducted to evaluate whether technical and non-technical students differed significantly in having security knowledge. Levene's test for equality of variances for H5 shows that Levene's *F* is statistically significant (Sig.≤ 0.05), then variances are significantly different and the assumption of "Equal variances not assumed" used for the test. The t-test results shows that significant difference was found in the scores of technical students (*M* =3.34, *SD* =.459) and non-technical students (*M* =3.18, *SD* =.433) conditions; t (420.3) = 3.876, p = 0.000. The results as shown in Table 4.5 suggest that there is a significant difference between knowledge level of technical and non-technical students. This ensures that technical students have more security knowledge.

Outcome	Student Group						95% CI for Mean Difference			
	Technical			Non – Technical						
	M	SD	n	M	SD	N			T	Df
Knowledge	3.3352	.45919	297	3.1756	.43252	190	.07866	.24049	3.876*	420.296

*$p < .05$.

Table 4.5 Results of T-tests and Descriptive Statistics Knowledge by Student Group.

After rejection of null hypothesis $H5_0$, we can calculate effect size. Effect size allows us to measure the magnitude of mean differences. We calculated the effect size using Cohen's formula as follows.

d = t sqrt ((N1 + N2)/N1N2)

d = 3.876 sqrt((297 + 190)/(297*190))

d = 0.355

The effect size for this analysis (*d* = 0.36) was found to lie between low (*d* = 0.2) and medium (*d* = 0.5) effect of Cohen's convention (1988). The students in the technical group scored 0.36 standard deviations higher in security knowledge than students in the non-technical group.

H6 : There is a significant difference between the attitude of technical and non-technical students.

Before testing the H6 hypothesis, we tested the six assumptions as tested before H5. Levene's test for equality of variances for H6 shows that Levene's *F* test is statistically significant (Sig.> 0.05) as shown in Table 4.6, then variances are significantly different that leads to consider the assumption of Equal variances assumed for the test.

		Levene's Test for Equality of Variances	
		F	Sig.
Attitude_R	Equal variances assumed	1.099	.295
	Equal variances not assumed		

Table 4.6 Levene's Test for homogeneity of variances for H6

Using an alpha level of .05, an independent – samples t-test was conducted to estimate whether technical and non-technical students' security attitude differed significantly. The t-test results shows that there was a significant difference in the scores of technical students (*M* =3.76, *SD* =.527) and non-technical students (*M* =3.49, *SD* =.494) conditions; *t* (485) = 5.636, *p* = 0.000. The results as shown in Table 4.7 suggest that there is a significant difference between attitude of technical and non-technical students. This ensures that technical students attitude towards security was better.

Outcome	Student Group						95% CI for Mean Difference			
	Technical			Non – Technical						
	M	SD	N	M	SD	N			t	Df
Attitude	3.7625	.52666	297	3.4933	.49389	190	.17532	.36302	5.636*	485

*$p < .05$.

Table 4.7 Results of T-tests and Descriptive Statistics Attitude by Student Group.

After acceptance of $H6_1$, we calculated the effect size using Cohen's formula.

d = t sqrt ((N1 + N2)/N1N2) = 0.524

According to Cohen's guidelines the calculation showed medium effect size (d=0.524). The results stated that students in the technical group scored 0.524 standard deviations higher in attitude towards security than students in the non-technical group. This means that students' attitude difference is greater than their knowledge magnitude difference. We can conclude that technical students' attitude towards security is better than non-technical.

H7 : There is a significant difference between the attitude of technical and non-technical students.

T-test assumptions are checked before conducting the analysis. Levene's test for equality of variances for H7 shows that Levene's F is statistically significant (Sig.> 0.05) as shown in Table 4.8, then variances are significantly different and Equal variances assumed was considered for the test.

		Levene's Test for Equality of Variances	
		F	Sig.
Behaviour_R	Equal variances assumed	.714	.398
	Equal variances not assumed		

Table 4.8 Levene's Test for homogeneity of variances for H7

Using an alpha level of .05, an independent – samples t-test was conducted to investigate whether technical and non-technical students' security behavior differed significantly. The t-test results shows that there was a significant difference in the scores of technical students (M =3.56, SD =.436) and non-technical students (M =3.40, SD =.448) conditions; t (485) = 3.990, p = 0.000. The results shown in Table 4.9 suggest that there is a significant difference between behavior of technical and non-technical students. This ensures that technical students' behavior towards security was better.

Outcome	Student Group									
	Technical			Non – Technical			95% CI for Mean Difference			
	M	SD	N	M	SD	N			t	Df
Behavior	3.5586	.43633	297	3.3952	.44786	190	.08293	.24387	3.990*	485

*p < .05.

Table 4.9 Results of T-tests and Descriptive Statistics Behavior by Student Group.

After acceptance of $H7_1$, we calculated the effect size using Cohen's formula.

d = t sqrt ((N1 + N2)/N1N2) = 0.371

According to Cohen's guidelines calculation showed low effect size (*d*=0.37). The results stated that students in the technical group scored 0.37 standard deviations higher in behavior towards security than students in the non-technical group. This means that students' behavior difference is less than their attitude magnitude difference. We can conclude that technical students' behavior towards security showed low difference than non-technical. This means that only knowledge does not help in improving behavior of students. It does not helped in producing large impact on their behavior. As also evident in a study by Halvei *et.al.*, 2016 that openness personality trait individuals found to have higher self-efficacy to handle security than the secure behavior.

4.3 Discussion

In the current study we proposed a research model comprises of individual, cultural and environmental factors. We used a quantitative methodology, involving the students from different institutes of NUST through survey and analysis of data in SPSS 22. After performing the statistical analysis as discussed in Results and Analysis section, we found that among five personality traits, openness showed a highly significant relationship with ISA. Openness trait as defined by McCrae and Johns, 1992 consist of attributes like creativity, flexibility, active imagination and appreciation towards new experiences and different ideas. The regression analysis showed that among our students openness trait showed significant result which can be used in awareness program interventions. This result was partially aligned with the literature review. In a study by Pattinson *et.al.*, 2015, individual factors like age, gender and personality differences influence on self-reported information security behavior was studied. The analysis concludes that agreeableness, openness, conscientiousness, ability to control impulsivity and age showed divergence in Information Security behavior. McCormac *et.al.*, 2017 analysis found that conscientiousness, agreeableness, emotional stability from the big five personality traits and risk taking propensity showed significant influence on individual's ISA. Halvei *et.al.*, 2016 found openness to be strong predictor of self-efficacy to handle security. These arguments support the acceptance of our hypothesis that openness has positive influence on individuals' ISA. As in

regression analysis, significant positive influence of openness found on ISA. In a study by Uebelacker and Quiel, 2014 openness leads to higher susceptible to social engineering attacks. These contradicting results emphasize the need of further research required to study the personality traits role in information security field. Which is also pointed out by Hu *et.al.,* 2012 that personality research has not been fully investigated in information security context. Halvei *et.al.,* 2016 also considered the analysis of personality attributes as a leap in improving cyber-security. Hu *et.al.,* 2012 found strong indication that personality could play a significant role in compliance behavior. Shropshire *et.al.,* 2015 also emphasized that personality traits help in filling the gap between intention and behavior by determining the user intention to engage in secure behavior. Individualized training programs coordinated as per personality and learning style, can be fruitful to maximize the result of the program (McCormac *et.al.,* 2017).

Shropshire *et.al.,* 2006 study showed that the traits of conscientiousness and agreeableness strongly linked with an individual's intention to comply with policies. Which is also described in a study by Russell *et.al.,* 2017, that conscientious individuals are more likely to engage in secure cyber behavior. McCormac *et.al.,* 2017 analysis found that conscientiousness, agreeableness, emotional stability from the big five personality traits and risk taking propensity showed significant influence on individual's ISA. However our results suggest the opposite. That is, conscientiousness and agreeableness does not have significant influence on individuals' ISA. According to Big 5 model by McCrae and Johns, 1992, conscientiousness trait described as self-discipline, self-control and dutifulness as well as following standards and rules. If we keep rule following characteristic of conscientiousness in mind, then we can consider the result of rule following hypothesis analyzed in the current study. As our result also showed the negative influence of rule following on ISA. Which conclude that making the rules for students to follow in order to keep up the security behavior is not helpful in influencing them towards security. Students are not inclined towards obedience of rule and regulation, which could be due to openness trait as a dominating personality dimension found in our sample. Openness trait as defined by McCrae and Johns, 1992 consist of attributes like creativity, flexibility, active imagination and appreciation towards new experiences and different ideas. By critically analyzing the information security compliance behavior and creativity, Hu *et.al.,* 2012 described the information security compliance behavior in terms of "follow the rules" behavior. Such behavior does not invoke creativity, thought processes or critical thinking. That means rule following behavior contradicts the openness personality characteristics. Keeping the rule following characteristic of conscientiousness and openness as dominant dimension of our sample in mind, conscientiousness insignificant influence on ISA could be understandable.

Agreeableness includes traits like cooperation, trustfulness, helpfulness and straightforwardness (McCrae and Johns, 1992). Shopshire *et.al.,* 2015 found agreeableness and conscientiousness as positively related to intent to use and actual use of security software. McCormac *et.al.,* 2017 also found significant impact of agreeableness on ISA. But in a study by Uebelacker and Quiel, 2014 who predict agreeable persons as more vulnerable to social engineering attacks due to their trust

factor. They suggested awareness trainings in the form of storytelling for agreeable individuals as prevention strategy. These arguments support rejection of hypothesis that agreeable individuals have positive influence on ISA. In our study the regression analysis showed insignificant influence of agreeableness on ISA. Which means that agreeableness factor is not helpful in improving ISA of students.

Interestingly, and contrary to our hypothesis, neuroticism was negatively correlated and showed insignificant influence on ISA. Neuroticism described in Big 5(McCrae and Johns, 1992) as tendency to experience negative emotions, anxiety and stress. McCormac *et.al.,* 2017 found neuroticism as a significant variant of ISA along with conscientiousness, agreeableness and risk taking propensity. In a study by McBride *et.al.,* 2012, while analyzing Big 5 personality traits as direct determinant of intention – neurotic individuals are less likely to violate cybersecurity policies. Which is logically aligns with the description of neurotic individuals as anxious and worrisome. This also evident in a study by Uebelacker and Quiel, 2014 which found neurotic individuals less susceptible to social engineering attacks like phishing due to being cautious. But in a study by Russell *et.al.,* 2017, the neurotic individuals are more likely to engage in insecure behavior. They have concluded it by relating the high level of anxiety and worrisome with the limited devotion towards cybersecurity. They observed positive significant correlation of depression, aggression and trait anxiety with insecure behavior. That leads to the conclusion that neurotic individuals are less likely to practice secure behavior. These arguments support our rejection of hypothesis $H1_d$ that a neurotic individual have positive influence on ISA. Analysis revealed that neuroticism has negative and insignificant correlation with ISA. Furthermore, regression analysis revealed that neuroticism does not have significant influence on ISA.

According to Big 5, extrovert individuals have positive emotions, more social, ambitious and excitement seeking behavior. Our hypothesis was rejected by having insignificant influence of extraversion on ISA. Extrovert participants analysis by McBride *et.al.,* 2012 also found them more inclined toward violating the cybersecurity policies while analyzing Big 5 as direct determinant of intention. Uebelacker and Quiel, 2014 also found extroverted individuals as more susceptible to social engineering attacks. Due to their sociability trait, they tend to more easily trapped by social engineering attacks based on the tactics of liking and social proof. Uebelacker and Quiel, 2014 suggested rewards as a prevention strategy for extraverted individuals while addressing the human factors in social engineering attacks. Halevi et.al., 2017 found insignificant relationship of extraversion and agreeableness with factors that influence security and privacy. They found personality traits, demographics and education as better predictors of security behavior and self-efficacy. Their study showed that personality traits affect users' cybersecurity behavior across different cultures which support the idea of developing personality based UI design (Halevi et.al., 2017). McCormac *et.al.,* 2017 also found insignificant relationship between Extraversion and ISA. These arguments support the rejection of hypothesis H1that extraversion have positive influence on ISA. Extraversion showed negative relationship with ISA and negative insignificant influence on ISA. Which means that extraverted individuals does not

influence individuals ISA. These arguments also highlight the importance of personality traits in the information security behavior and intervention strategies as per personality traits to improve the security behavior.

Furthermore, regression analysis revealed that openness, age, secondary source influence, peer pressure and rule following significantly explain variance in ISA. The environmental construct comprises of factors, secondary source influence and peer pressure as primary source of influence was used in current study. Peer pressure showed significant but negative influence on ISA through regression analysis. This shows that peer pressure is unable to improve security behavior of students because of not having security culture in institutes. But significant relation of peer pressure with ISA will show positive results when organizations have security culture of following security policies and practices. Peer pressure and secondary sources influence on ISA also evident in a study by Haeussinger, 2013. Peers' information security behavior seems to be influenced by others' opinion and perception about information security behavior. Means, if an individual perceived that his or her coworkers or friends were using a particular IS safeguard, the individual inclined to follow his behavior. Which shows that peer influence makes an individual consciously or unconsciously behave according to the common practices being followed in their organization (Karjalainen *et.al.,* 2013). Veiga & Martins, 2015 empirically evident that training and awareness has a positive impact on the security culture of an organization and employee behavior could be directed toward corrective actions.

Herath & Rao, 2009 suggests that the expectations of superiors, peers seem to have strong influence on employee security behaviors. Not only the expectations but the perceived behavior of others, was found to be a factor with significant influence on employee intentions to comply with the policies. Managers can increase security compliance by improving the security culture in their organization (Herath & Rao, 2009). Our results also reflect that peer pressure positive influence will show its effects, when security culture has been established in an organization. Employees' misbehavior and risks to information assets can be minimized by establishing security culture in an organization (Da Veiga and Eloff, 2010).

Secondary sources (newspaper, radio, internet and TV) information from multiple sources showed positive impact on ISA. Karjalainen *et.al.,* 2013 also evident that the prominence of information security in the media showed an impact on employees' security behavior. Media richness in ISA interventions other than the traditional channels and comprehensive mix of IS interventions will lead to improved compliance behavior towards information security policies (Bauer *et.al.,* 2017). Awareness programs need to take into account the strategies which can influence these environmental factors as well.

The culture factor we took in this study was used to investigate the organization culture effect on ISA. As suggested by Karjalainen *et.al.,* 2013, different cultures require different interventions for changing employee behavior towards information security. Organizations need to customize their IS security interventions and practices to adjust according to the cultural and local needs.

Da Veiga, 2016 defined cybersecurity culture at different levels starting from individual to organizational, national to international levels – which includes all devices and people that are connected globally. Organizational culture mostly defined as "the way we do things here" (Lundy & Cowling, 1996). Muijen *et.al.,* 1999 described the organizational culture in terms of four basic values: support orientation, innovation orientation, goal orientation, and rule orientation. Hu *et.al.,* 2012 used the goal and rule orientations of Muijen, 1999 to study the role of organizational culture and top management in shaping compliance behavior.Hu found that top management involvement strongly influences the organizational culture which impacts the employee attitude and behavior towards compliance with information security policies. They provided practical insights for designing workplaces that inspire self-regulation and foster rule adherence among employees (Hu *et.al.,* 2012). In the current study, we took the rule following variable to investigate institutions culture. The result of rule following variable showed significant but negative relation with ISA, rule following negatively influences ISA. Which means that the more students dragged towards rules the less their ISA will be. Rule formation would not help in improving users' attitude or behavior towards security. As mentioned by Hu *et.al.,* 2012 that rule following behavior does not invoke creativity, thought process or critical thinking which supports our hypothesis results that students with openness to experience will not be inclined to follow the rules as per their personality dimension. Halevi *et.al.,* 2016 also concluded through results that personality traits affects individual security behavior across different cultures. Another assumption could be derived as the role of top management in influencing organizational culture which impacts employees' compliance behavior (Hu *et.al.,* 2102). Lack of interest of the NUST management toward information security could be the factor behind the non-compliant attitude of students. Top management can influence employee behavior through active participation in information security initiatives (Hu *et.al.,* 2102).

Information security awareness measured in this study using the KAB model in three dimensions knowledge, attitude and behavior (Kruger & Kearney, 2006, Parsons *et.al.,* 2014).HAIS-Q measuring instrument by Parsons *et.al.,* 2014 was used to measure the overall information security awareness of students. Parsons *et.al.,* 2014 emphasized that training and education effectiveness will be evident when user not only have the knowledge but understand why they need and how it will benefit them. In our study, significant difference was found in knowledge level of technical and non-technical students. But the magnitude of difference was not that much significant in the attitude and behavioral differences among technical and non-technical students as discussed in Results and Analysis section. This shows that only knowledge is not helpful in changing attitude and behavior of students towards information security. It is also evident that only knowledge of concepts didn't refrain an individual from indulging in unprotected practice (Stanciu & Tinca, 2016, Chan & Mubarak, 2012). Pattinson *et.al.,* 2015 in an empirical study also found unexpectedly that those employees who are less familiar with computers are likely to be less risky to unknown malicious behavior. Security knowledge alone is not helpful in increasing security practices understanding even in educational institutes, security policies, continuous awareness and training is vital to create security impact at organizational level

(Ramalingam *et.al.*, 2016). Ismailova & Muhametjanova, 2016 also found that students from technical field are not different from non-technical in terms of awareness of internet risks.

4.4 Problems in NIST Awareness program model

As discussed above only imparting knowledge is not enough to influence behavior of students towards security. Security awareness programs need to cater behavioral aspects for getting the practical results. Stewart & Lacey, 2012 also pointed out that NIST awareness model (SP 800-50) as shown in Figure 4.3 was found to be as "broadcast of facts". It only focuses on technical competencies and ignores factors like demographics, culture and existing beliefs. It provides constricted view of requirements in needs assessment by only focusing on the tasks audience need to perform. To make information security awareness techniques effective, contents of awareness material should not be based on what technical experts wants to tell people but on what will influence the audience. They highlighted the necessity to improve requirement extraction process through needs assessment in security awareness program.

Tsohou *et.al.*, 2015 also discussed that Security standards and guidelines e.g. NIST and ENISA, do not take into consideration whether knowledge of the awareness material will actually results in improved security behavior. Awareness programs need to go beyond the simple communication of facts and figures, we need to influence users' security behavior as well. Awareness programs lack in formulating users' perception about security and highlighted the need to alter awareness strategies. Security management strategies need to emphasize on how to boost the security behavior besides recognizing what behavior needs to be influenced. Author also pointed out that existing standards like NIST 800 – 50, 2003 or ENISA, 2010 take into account the business needs as per culture of the organization but they didn't consider(tackle) personal belief, attitude or biases mediating effect on security awareness. They explored the role of cognitive and cultural biases in influencing security perceptions and behaviors. By further highlighting the shortcomings in existing awareness program development phases like planning, development and implementing, recommendations are provided for alleviating(improving) the effect of cognitive and cultural biases on security behavior. In planning phase of standards like NIST and ENISA, identification of target groups is performed on the basis of users' role and knowledge, without taking into consideration individual attitude, traits or biases. Needs assessment activity can be improved by providing an alternative criteria on the basis of cultural biases for identifying target group. Formulation of communication plan can be improved by selecting awareness topics, sources and deployment methods on the basis of cultural biases. Cultural biases can also show its influence on senior management perceptions which could be helpful in decision making regarding awareness program's budget and program's needs and risks. In development phase, cultural biases effects can be seen by using positive stimuli, reliance on first piece of information and immediate application of sanction while security awareness material development. In implementation phase, cultural or cognitive biases influence can be seen positively by comparing current practices with alternative options. Security practices should be strong enough that it can easily engage the users and they can easily be remembered. Authors

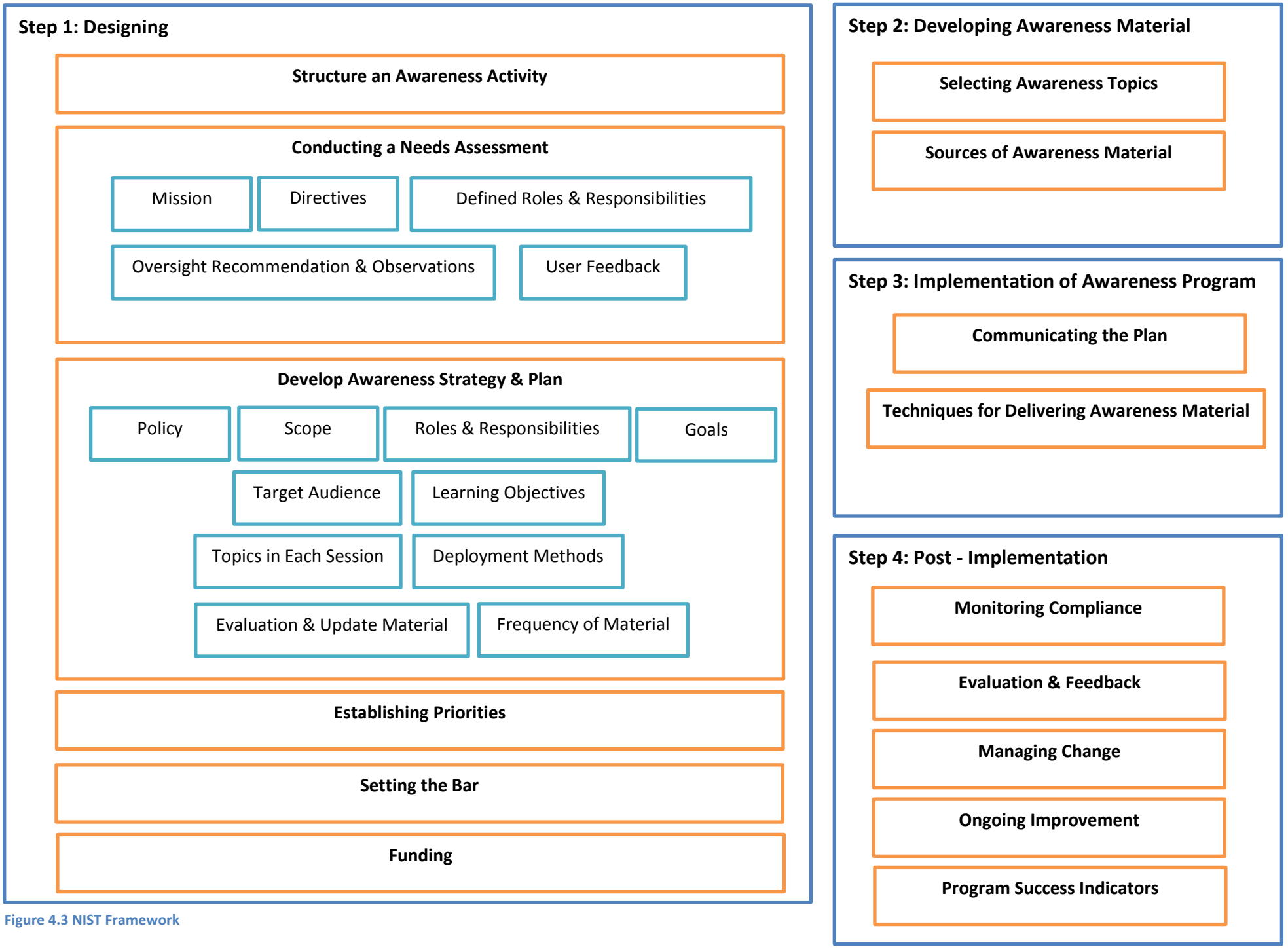


Figure 4.3 NIST Framework

claim that these recommendations don't demand extra resources but direct management towards strategic choices.

4.5 Addressing deficiencies in NIST Awareness program model

After highlighting the shortcomings in awareness program model in previous section, we improved the model by addressing the deficiencies through interventions as per individual, cultural and environmental factors result as shown in Figure 4.4.

During design phase, activities carried out by security managers include: needs assessment, programs goal and objectives, target audience identification, deployment methods, setting priorities and funding of the program. In needs assessment the target audience are identified as per their role and responsibilities without taking into consideration their personality traits. Personality analysis of target audience would be helpful in identifying strategies which will influence user behavior according to their personality. Personality traits showed significant impact on ISA and they can be used to develop tailored security awareness programs or training (McCormac *et.al.,* 2017). To examine the human aspect of information security, personality traits analysis would be effective for understanding their personality effect on security behavior (Pattinson *et.al.,* 2015). Personality analysis in design phase would be further helpful in developing and implementing awareness program while keeping in mind the personality of audience. This intervention will be helpful in rectifying the problem identified by Stewart & Lacey, 2012 that information security approaches are fact focused not audience focused.

In planning and strategy development, with topic and deployment method selection, secondary sources of information can be selected as per the environmental requirements of the organization. Information received from secondary sources highlight potential risks and the importance of information security which positively impacts awareness. Positive impact of secondary source information on users' knowledge and behavior improve their ISA (Haeussinger, 2013). Mass media (newspaper, TV, Internet, radio) as an external factor influences the user's intention to practice security and persuade individual towards compliance (Ng & Rahim, 2005; Siponen *et.al.,*2009). The reflection of information security through media leaves an impact on security behavior of employees. Those employees who are susceptible to security concerns likely to comply with security policies due to close engagement with media (Karjalainen *et.al.,* 2013). Media richness was also emphasized by Bauer *et.al.,* 2017 for IS interventions. Positive influence of SSI can be used to boost the security culture within an organization. We emphasized the role of SSI by making it part of the strategy plan of the program.

Once the awareness program has been designed, the awareness content can be developed while keeping in mind what behavior we want to reinforce and what skills audience needs to apply. In the development phase, awareness topics and sources of awareness material are selected (NIST 800-50, 2003). NIST provides a list of topics (e.g. password, spam) and communication means (e.g. E-mail, periodicals). Stewart & Lacey, 2012 explained that general presentation of facts is a constricted view of risk communication that results in ineffective communication. Only knowing

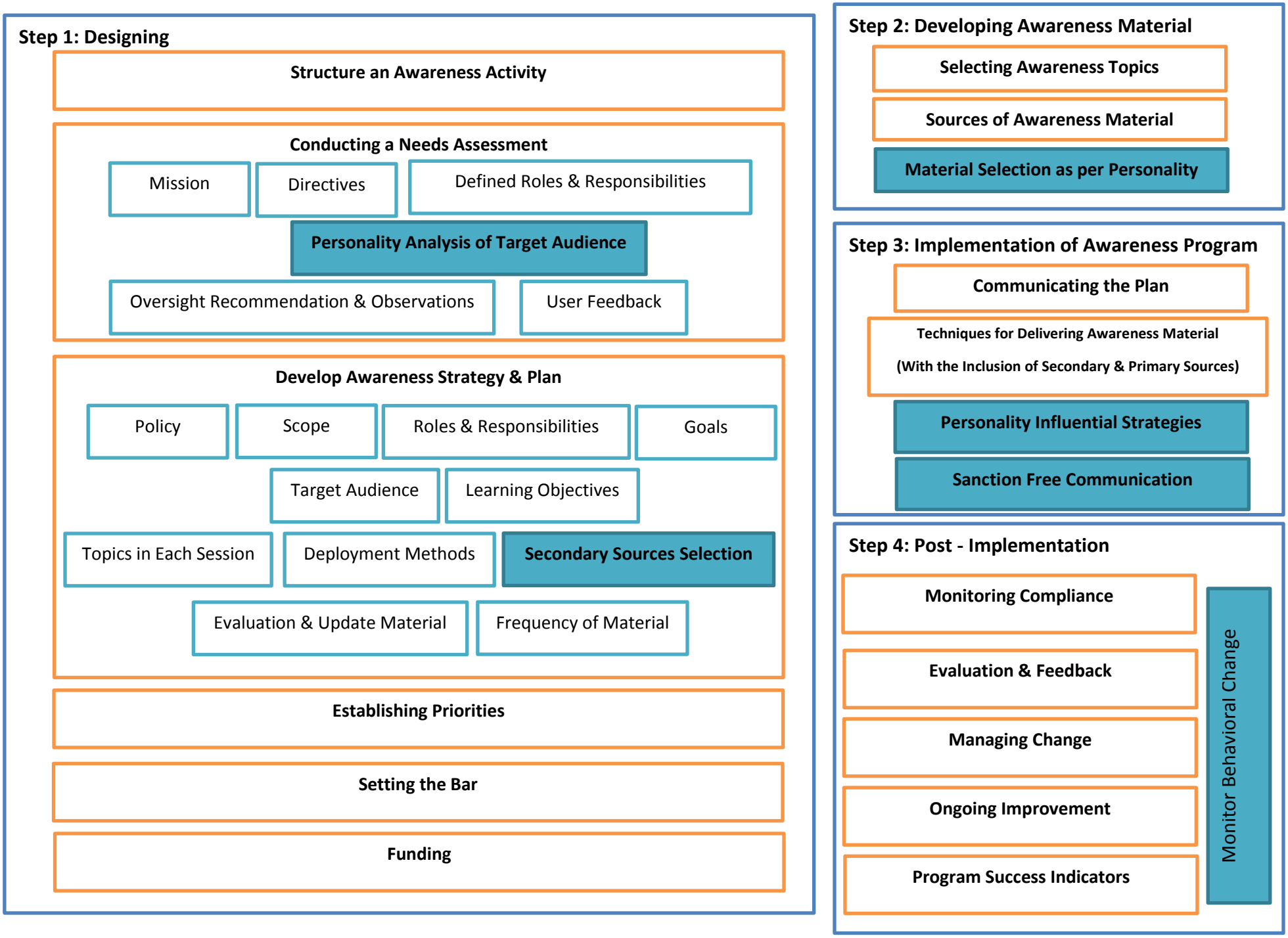


Figure 4.4 Modified NIST Framework for Awareness Program

the behavior which is causing the security risks is not enough, why the behavior is occurring must be understood by the communicators. This requires focus on identifying and influencing audience's constraints and supporting beliefs. Awareness material can be developed according to personality which will influence users more powerfully than simple communication. Kajzer *et.al.,* 2014 also evident that effectiveness of security awareness message vary based on personality. Some security messages appear beneficial and some seems less effective according to personality traits. Security awareness and behavioral change interventions can be developed more effectively by taking into account the personality traits and thinking styles of users (Kajzer *et.al.,* 2014). Tailored awareness material designed according to the personality of audience will be more effective than uniform content across a user population. Personalized ISA could increase personal ownership and vigilance toward security (Ahlan *et.al.,* 2015). Stewart & Lacey, 2012 also stressed that for improving the effectiveness of security awareness techniques, awareness content cannot be created to satisfy what technical experts want to tell but the audience that it seeks to influence.

In implementation phase, after communicating the plan, techniques of delivering awareness material is selected depending on the resources and complexity of messages. NIST 800-50 provided a list of techniques that can be used to disseminate the message. NIST only emphasized the selection based on availability of resources and the number of messages to deliver information. Delivery techniques with inclusion of secondary and primary sources will be more effective in communicating message. As discussed above primary sources' of influence include peers, friends and family members and co-workers. While secondary sources' of influence include mass media coverage such as newspaper, TV, Internet(Brown & Venkatesh, 2005). The positive impact of secondary source information and peer influence on IS behavior have stronger effect on compliance (Karjalainen *et.al.,* 2013, Manke & Winkler, 2012). Using secondary and primary sources while selecting delivery techniques e.g. poster, discussion, seminar will be helpful in improving the ISA level. Secondary sources and real life stories sharing by peers and seniors will be helpful in involving user in awareness activities (Bauer *et.al.,* 2017).Safa *et.al.,* 2016 study revealed that information security knowledge sharing, collaboration, intervention and experience have an influential impact on employees' attitude towards compliance with information security policy of organization. Knowledge sharing, collaboration, intervention and experience depict different aspects of involvement. Involvement showed its influence on attitude through these different aspects. Information security knowledge sharing in an organization is an effective approach to increase not only the level of awareness but it depicts the user involvement in information security. The use of secondary and primary sources to share knowledge among participants will be helpful in improving their attitude towards security. Attitude towards compliance will be helpful in effecting the behavioral intention regarding information security compliance (Safa *et.al.,* 2016).

To further improve the effectiveness of awareness model, we included the personality influential techniques in implementation phase. Organizational efforts seem to face failure due to

negligence to focus on individuals (Webb *et.al.,* 2014). Focusing on audience and selecting influential techniques according to their personality can improve the results of awareness programs. Big five model reflects aspects of human personality and have influence on individual ISA (McCormac *et.al.,* 2017, Pattinson *et.al.,* 2015). As in our study the openness was the dominating factor in students' personalities, inclusion of those techniques which can exploit their openness will increase the effectiveness of awareness program. In a study by Barrick & Mount, 1991 Openness to experience trait showed positive attitude towards learning experiences and it seems to be valid predictor of training proficiency. Individuals who score high on this dimension are more likely to benefit from training as individual attitude is a key component in the success of a training program (Barrick & Mount, 1991). Through literature analysis, we have recorded group discussion, positive feedback and reward as influential strategies for openness personality trait. In a study by Komarraju & Karau, (2005), they found that students with openness and extraversion personality dimensions are more engaged in learning. They suggested that such students would take more benefits from discussion and interactive learning because they are more social and enjoy exposure to new ideas. They also suggested that to increase engagement and achievement level of students with the qualities of openness and conscientiousness, rewarding strategy would be beneficial to force them think beyond the boundaries of the topic. Discussion by role models as creative and interactive approach would be helpful in involving users emotionally as evident in a study by Bauer *et.al.,* 2017. George & Zhou, 2001 suggested that positive feedback can be vital for encouragement of creative behavior among individuals who perform experimental tasks and high on openness to experience. Educators or communicators need to select activities and delivery mode as per personality preferences of students (Komarraju & Karau, 2005). Practice of using personality modeled influential techniques would be helpful in influencing behavior of individuals.

For organizations to be successful employees must follow rules and policies. Employees often break or bend the rules that conflicts the working expectations (Hannah & Robertson, 2015). As in our study, rule following variable showed significant but negative relation with ISA. This shows that rule formation is not influencing students' behavior toward security. Based on this result we included sanction (command) based/free communication as a component which needs to be taken into consideration in implementation phase. Making rules and expecting students to follow the rules will not helpful in increasing their compliance. Our investigated participants are high on openness to experience, creative, curious, adventurous, value change, and intellectual (Barrick & Mount, 1991). Based on the definitions, openness personality trait share similar characteristics as openness to change moral values (Myyry *et.al.,* 2009). Based on this context, these people do not respect rules and they prefer to follow their own intellectual and emotional interests (Bardi & Schwartz, 2003). Such individuals display critical attitude towards information security rules and policies (Myyry *et.al.,* 2009). Hu *et.al.,* 2012 also pointed out that creative individuals are less inclined towards rule following behavior. Depending on the personality of users, organization should select whether to choose sanction, enforcement style or rewarding and appreciative (command based or command free) style for communicating awareness material.

For our case study we will select command free style of communication as openness make them less prone to feeling guilty over disobedience (Silfver *et al.,* 2008). Organization prefer those individuals who are more open to novelty, creative, and self-directed rather than those who act based on fear of sanctions (Myyry *et.al.,* 2009). In one of the case studies by Bauer *et.al.,* 2017, they also highlighted the negative influence of directive messages on users by creating irritation. Awareness programs customized according to culture differences and user groups will be helpful in influencing their behavior (Tsohou *et.al.,* 2015, Bauer *et.al.,* 2017).

After suggesting all the additions in awareness program model to improve behavior towards security, post implementation phase needs to monitor behavioral change. For continuous improvement, we need to check the effectiveness of techniques. For measuring behavioral change, survey questionnaire, quizzes and feedbacks are the most efficient ways. These approaches invoke user involvement and validate the usefulness of IS interventions (Bauer *et.al.,* 2017). Feedback interventions can be helpful in enabling effective two way communication (Bauer *et.al.,* 2017). Evaluation seems vital for on-going improvement of ISA programs and its resulting effect among users. Adjustments of an ISA program based on evaluation results lead to improved levels of behavioral IS compliance (Bauer *et.al.,* 2017).

4.6 Awareness Program Model for SEECS

After giving the holistic view of the ISA model, we developed a model for SEECS institute using an Ad hoc approach. In this model we targeted only one institute of NUST according to scope of our study. As students of SEECS have technical background and they study courses related to information technology and security. Based on their technical background, we suggested developing a team of volunteer students as SEECS have one named as ACM (Association for Computing Machinery). This team with the ISA manager (e.g. member of student affairs) will work together for developing and implementing awareness program. The components of awareness program model shown in Figure 4.5 are as follows:

4.6.1 Design and Development Phase:

In this phase the ISA team will develop the awareness material according to the requirements which will be identified through needs assessment. In needs assessment, the team will follow the steps specified in our modified NIST awareness framework. Depending on the requirements collected through needs assessment, the team will develop the awareness material. Awareness material will be developed in context of participants' personality and their technical background and knowledge level. Awareness material will be approved by the ISA manager. After getting approval, team will schedule the awareness session and events. Schedule approval will also be sought from the manager. In case of not getting approval for awareness material and schedule, team will make the required changes to get the approval.

Awareness Program Model

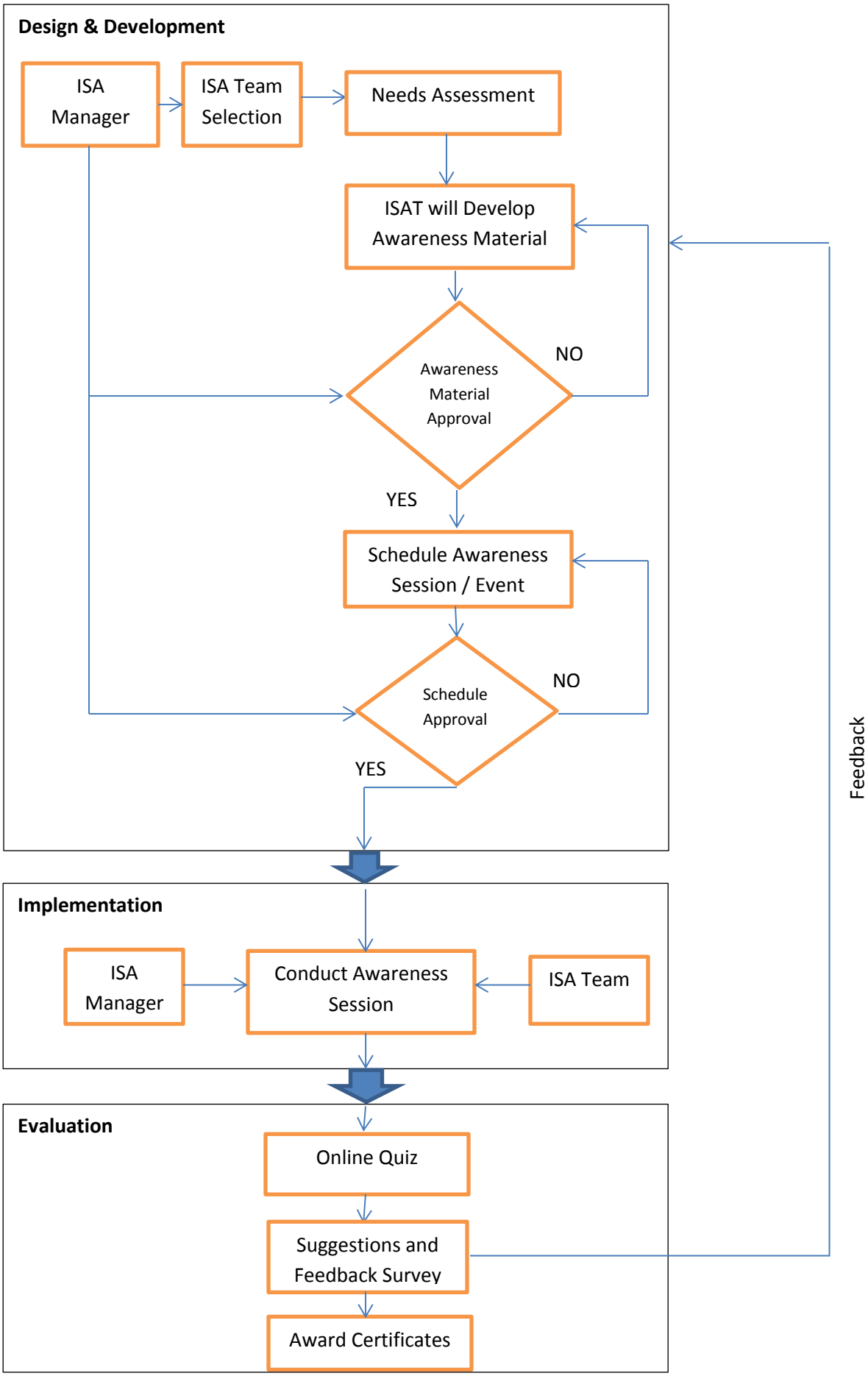


Figure 5.2 Awareness Program Model for SEECS

4.6.2 Implementation Phase:

In this phase ISA team will conduct the session under the supervision of manger. As in our study the openness emerged as dominating personality dimensions among students. From literature review we have seen that influential strategies for openness are discussion, positive feedback and reward. Primary and secondary sources can be selected for having better impact on their behavior. On the basis of needs assessment results, implementation strategies will be selected for conducting the session or event.

4.6.3 Post-implementation / Evaluation Phase:

To monitor the effectiveness of the awareness program, we suggested the online quiz and suggestions and feedback surveys. These evaluation strategies are beneficial for evaluating behavioral change. On the basis of quiz results students can be rewarded by awarding certificates of the attended session. By introducing certificates, we are influencing the students as per their openness personality trait. One can use rewards according to their budget and management support.

This ad hoc model is feasible for an institute on small scale and its scope can be increased by adding more techniques and by targeting more personality traits and influential strategies.

Summary:

We have investigated the individual, environmental and cultural factors effect on ISA of students. On the basis of statistical analysis, we incorporated new components into ISA framework to improve the deficiencies in NIST security awareness framework. These components have been selected on the basis of personality, environmental and organization culture influence on students' security behavior. We also provided an ad-hoc model for one of the institutes of the target organization.

CHAPTER 5

Conclusion & Future Work

This chapter concludes the presented thesis and highlights potential future research directions in the domain of information security awareness. The first section of the chapter gives a brief conclusion of the major research contributions, whereas second section presents the future research work directions.

5.1 Conclusion

This study investigated the relation among individual, environmental and cultural differences and information security awareness. ISA was computed by using the HAIS-Q (McCormac, 2017). HAIS-Q was used to analyze the relation between knowledge of security policy and procedures, attitude towards policy and procedures and behavior in a working environment (Parsons et.al., 2014). As their findings suggested that training and education will be more effective if it not only provide knowledge but also provide an understanding of its importance which will improve their behavior towards security. As McCormac highlighted that for investigating the user awareness effect on information security, it is essential to understand individual differences among individuals. To interpret differences among individuals, psychology behind individual variance need to be understood. This information can be used to tailor awareness or training programs to improve ISA.

This study examined the relationship of individual, environmental, cultural factors and information security awareness. We analyzed and investigated the collective impact of environmental, cultural and individual factors on information security behavior of an individual. Personality traits, individual distinguishing variable as per their psychology showed a significant influence on ISA. In our case study of NUST students, openness to experience personality dimension showed a significant variance in individuals' ISA. Environmental factors, peer pressure and secondary source influence showed a significant positive impact on ISA. Cultural factor, rule following showed a significant but negative relation with ISA due to lack of security culture in the organization.

Our study also filled the gap in awareness programs to effect the behavior by highlighted the deficiencies in the existing awareness programs and by adding the components in awareness program which could have influential effect on behavior of target audience. We improved the NIST awareness program framework by strategically influencing the individual, environmental and cultural factors. Our modified framework could help organizations to have a tailored awareness program as per their organizational culture, environment and personality of the target audience. The addition of personality modules could improve the effectiveness of awareness program by targeting and improving the behavior of an individual. The personality analysis

would help organizations to target discrepancy between behavioral intentions and actual behavior. The addition of modules on the basis of analysis of environmental and cultural factors would further enhance the effectiveness of the framework by optimizing it as per their organizational culture and peers influence.

We also developed an awareness program model for SEECS institute using an ad hoc approach. This ad hoc model will process according to the improved NIST awareness program framework. Through development, implementation and evaluation phases, the utilization of framework components will enhance the behavioral outcomes of the model.

5.2 Future Work

In our study we provided a holistic view of the awareness program model. Due to time limitations we couldn't implement the model so we provided the ad-hoc model for one of the technical institutes of NUST. In future we could implement the awareness program in different departments of NUST and analyze the actual change in behavior of students. To investigate the effectiveness of the awareness program we could perform the post survey to analyze change in students' knowledge, attitude and behavior towards information security.

Future research could discover and analyze ISA interventions according to the different types of personalities. For each type of personality, ISA interventions and influential strategies need to be investigated and evaluated through empirical studies. In our study we only searched the openness personality dimension as the dominating factor in our studied population. We investigated the influential strategies according to our targeted audience. The effectiveness of these personality influential strategies could be measured by implementing the awareness program and evaluating its influence on students' behavior by monitoring change in their behavior. The evaluation of the awareness program model could be performed through qualitative research. Qualitative study could more accurately identify the effects of awareness program on students' attitude and behavior.

In future we could investigate the role of top management in analyzing its' influence on organizational culture (Hu *et.al.,* 2012). Which could be helpful in analyzing other than personality traits influence, the influence of top management behavior its effect on students' attitude toward rule following.

Summary:

This chapter has presented the conclusion of our thesis, highlighting the major research contributions. Furthermore, it describes potential future directions in which our thesis can be extended for further research work.

Appendix A: Survey Questionnaire

SECTION A: Demographic Data

Gender:	☐ Male	☐ Female		
Age:	☐ (18 or Under)			
	☐ (19 – 24)			
	☐ (25 – 31)			
	☐ (32 – 38)			
	☐ (39 or Above)			
Institute:	☐ SEECS	☐ MCS	☐ IGIS	☐ _____
Degree:	☐ Bachelors	☐ Masters		
Discipline: (e.g. BEE)	_____	Semester:	_____	

SECTION B: Survey

The following statements concern your perception about yourself in a variety of situations. Please encircle the appropriate box against each statement to indicate the extent to which you agree or disagree with the statement by using the following scale.

	I see myself as someone who...	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	Does a thorough job.	1	2	3	4	5
2.	Is communicative, talkative.	1	2	3	4	5
3.	Is sometimes somewhat rude to others.	1	2	3	4	5
4.	Is original, comes up with new ideas.	1	2	3	4	5
5.	Worries a lot.	1	2	3	4	5
6.	Has a forgiving nature.	1	2	3	4	5
7.	Tends to be lazy.	1	2	3	4	5

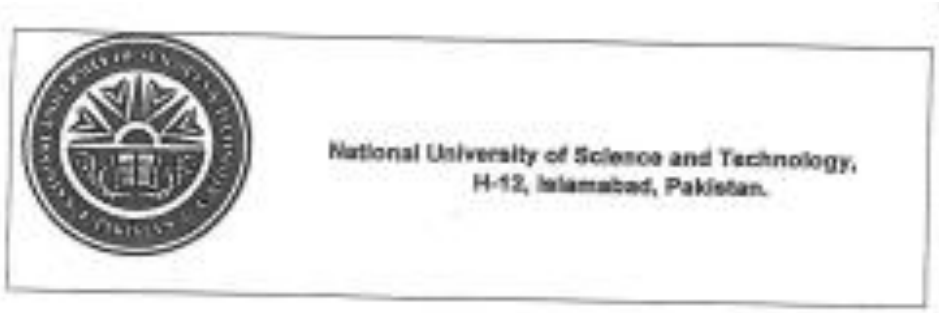
8.	Is outgoing, sociable.	1	2	3	4	5
9.	Values artistic experiences.	1	2	3	4	5
10.	Gets nervous easily.	1	2	3	4	5
11.	Does things effectively and efficiently.	1	2	3	4	5
12.	Is reserved.	1	2	3	4	5
13.	Is considerate and kind to others.	1	2	3	4	5
14.	Has an active imagination.	1	2	3	4	5
15.	Is relaxed, handles stress well.	1	2	3	4	5
	Password Management					
16.	It's acceptable to use my social media passwords on my other accounts.	1	2	3	4	5
17.	It's safe to use the same password for social media and other accounts.	1	2	3	4	5
18.	I use a different password for my social media and other accounts.	1	2	3	4	5
19.	It's acceptable to share my passwords with friends.	1	2	3	4	5
20.	It's a bad idea to share my passwords, even if a friend asks for it.	1	2	3	4	5
21.	I share my passwords with friends.	1	2	3	4	5
22.	A mixture of letters, numbers and symbols is necessary for passwords.	1	2	3	4	5
23.	It's safe to have a password with just letters.	1	2	3	4	5
24.	I use a combination of letters, numbers and symbols in my passwords.	1	2	3	4	5
	Email Use					
25.	It's acceptable to click on any links in emails from people I know.	1	2	3	4	5
26.	It's always safe to click on links in emails from people I know.	1	2	3	4	5
27.	I don't always click on links in emails just because they come	1	2	3	4	5

	from someone I know.					
28.	It's acceptable to click on a link in an email from an unknown sender.	1	2	3	4	5
29.	Nothing bad can happen if I click on a link in an email from an unknown sender.	1	2	3	4	5
30.	If an email from an unknown sender looks interesting, I click on a link within it.	1	2	3	4	5
31.	It's acceptable to open email attachments from unknown senders.	1	2	3	4	5
32.	It's risky to open an email attachment from an unknown sender.	1	2	3	4	5
33.	I don't open email attachments if the sender is unknown to me.	1	2	3	4	5
	Internet Use					
34.	It's acceptable to download any files onto my computer if they help me to do my job.	1	2	3	4	5
35.	It can be risky to download files on my computer.	1	2	3	4	5
36.	I download any files onto my computer that will help me get the job done.	1	2	3	4	5
37.	While I am at Institute, I shouldn't access certain websites.	1	2	3	4	5
38.	Just because I can access a website at Institute, doesn't mean that it's safe.	1	2	3	4	5
39.	When accessing the Internet at Institute, I visit any website that I want to.	1	2	3	4	5
40.	It's acceptable to enter any information on any website if it helps me do my job	1	2	3	4	5
41.	If it helps me to do my job, it doesn't matter what information I put on a website.	1	2	3	4	5
42.	I assess the safety of websites before entering information.	1	2	3	4	5
	Social Media Use					

43.	I will not be penalized for something I post on social media.	1	2	3	4	5
44.	It doesn't matter if I post things on social media that I wouldn't normally say in public.	1	2	3	4	5
45.	I don't post anything on social media before considering any negative consequences.	1	2	3	4	5
46.	I can post what I want about my Institute on social media.	1	2	3	4	5
47.	It's risky to post certain information about my Institute on social media.	1	2	3	4	5
48.	I post whatever I want about my Institute on social media.	1	2	3	4	5
	Secondary Source Influence					
49.	Based on what I have heard or seen on mass media (TV, radio, newspapers, internet), I am encouraged to follow information security best practices.	1	2	3	4	5
	Rule Following	Never	Rarely	Sometimes	Often	Always
50.	A website is blocked in your institute; will you open it (e.g. using proxy)?	1	2	3	4	5
51.	By rule, you are not allowed to make a page about your institute on social media. Would you bypass the policy by making an unofficial one?	1	2	3	4	5
52.	You are always suggested to change your default password (email, LMS, CMS). Do you follow this practice?	1	2	3	4	5
	Peer Pressure	Never	Rarely	Sometimes	Often	Always
53.	Your friend saved the password on his system. Will you do the same practice?	1	2	3	4	5
54.	Your friends have a group on social media and they posted	1	2	3	4	5

	something negative about the institute. Will you comment or share the post?					
55.	You and your friend received an email from a known/unknown sender. You don't want to open it but your friend did. Will you open it?	1	2	3	4	5

Appendix B: Filled Survey Questionnaires



National University of Science and Technology,
H-12, Islamabad, Pakistan.

Declaration

Dear Respondents,

I, student of NUST studying the behavioral and environmental factors effects on students' Information Security Awareness. I assure you that, strictly following the research ethics, your replies will be kept strictly confidential and the data acquired will only be used for academic research purposes. This information will not be disclosed to anyone and the data will be summarized on a general basis only.

SECTION A: Demographic Data

Gender:	☑ Male	☐ Female		
Age:	☐ (18 or Under)			
	☑ (19 – 24)			
	☐ (25 – 31)			
	☐ (32 – 38)			
	☐ (39 or Above)			
Institute:	☑ SEECS	☐ MCS	☐ EME	☐ IGIS
Degree:	☑ Bachelors	☐ Masters		
Discipline: (e.g. BEE)	BESE	Semester:	7th	

SECTION B: Survey

The following statements concern your perception about yourself in a variety of situations. Please encircle the appropriate box against each statement to indicate the extent to which you agree or disagree with the statement by using the following scale.

	I see myself as someone who...	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	Does a thorough job.	1	2	(3)	4	5
2.	Is communicative, talkative.	1	2	3	(4)	5
3.	Is sometimes somewhat rude to others.	1	(2)	3	4	5
4.	Is original, comes up with new ideas.	1	2	3	(4)	5
5.	Worries a lot.	(1)	2	3	4	5
6.	Has a forgiving nature.	(1)	2	3	4	5
7.	Tends to be lazy.	1	2	3	(4)	5
8.	Is outgoing, sociable.	1	2	3	4	(5)
9.	Values artistic experiences.	1	2	(3)	4	5
10.	Gets nervous easily.	1	(2)	3	4	5
11.	Does things effectively and efficiently.	1	2	3	(4)	5
12.	Is reserved.	1	(2)	3	4	5
13.	Is considerate and kind to others.	1	2	3	(4)	5
14.	Has an active imagination.	1	2	3	(4)	5
15.	Is relaxed, handles stress well.	1	(2)	3	4	5
	Password Management					
16.	It's acceptable to use my social media passwords on my other accounts.	1	2	3	(4)	5
17.	It's safe to use the same password for social media and other accounts.	1	2	3	(4)	5

18.	I use a different password for my social media and other accounts.	1	2	3	4	5
19.	It's acceptable to share my passwords with friends.	1	2	3	4	5
20.	It's a bad idea to share my passwords, even if a friend asks for it.	1	2	3	4	5
21.	I share my passwords with friends.	1	2	3	4	5
22.	A mixture of letters, numbers and symbols is necessary for passwords.	1	2	3	4	5
23.	It's safe to have a password with just letters.	1	2	3	4	5
24.	I use a combination of letters, numbers and symbols in my passwords.	1	2	3	4	5
	Email Use					
25.	It's acceptable to click on any links in emails from people I know.	1	2	3	4	5
26.	It's always safe to click on links in emails from people I know.	1	2	3	4	5
27.	I don't always click on links in emails just because they come from someone I know.	1	2	3	4	5
28.	It's acceptable to click on a link in an email from an unknown sender.	1	2	3	4	5
29.	Nothing bad can happen if I click on a link in an email from an unknown sender.	1	2	3	4	5
30.	If an email from an unknown sender looks interesting, I click on a link within it.	1	2	3	4	5
31.	It's acceptable to open email attachments from unknown senders.	1	2	3	4	5
32.	It's risky to open an email attachment from an unknown sender.	1	2	3	4	5
33.	I don't open email attachments if the sender is unknown to me.	1	2	3	4	5
	Internet Use					
34.	It's acceptable to download any files onto my computer if they help me to do my job.	1	2	3	4	5
35.	It can be risky to download files on my computer.	1	2	3	4	5

36.	I download any files onto my computer that will help me get the job done.	1	2	3	4	5
37.	While I am at Institute, I shouldn't access certain websites.	1	2	3	4	5
38.	Just because I can access a website at Institute, doesn't mean that it's safe.	1	2	3	4	5
39.	When accessing the Internet at Institute, I visit any website that I want to.	1	2	3	4	5
40.	It's acceptable to enter any information on any website if it helps me do my job	1	2	3	4	5
41.	If it helps me to do my job, it doesn't matter what information I put on a website.	1	2	3	4	5
42.	I assess the safety of websites before entering information.	1	2	3	4	5
	Social Media Use					
43.	I will not be penalized for something I post on social media.	1	2	3	4	5
44.	It doesn't matter if I post things on social media that I wouldn't normally say in public.	1	2	3	4	5
45.	I don't post anything on social media before considering any negative consequences.	1	2	3	4	5
46.	I can post what I want about my Institute on social media.	1	2	3	4	5
47.	It's risky to post certain information about my Institute on social media.	1	2	3	4	5
48.	I post whatever I want about my Institute on social media.	1	2	3	4	5
	Secondary Source Influence					
49.	Based on what I have heard or seen on mass media (TV, radio, newspapers, internet), I am encouraged to follow information security best practices.	1	2	3	4	5
	Rule Following	Never	Rarely	Sometimes	Often	Always
50.	A website is blocked in your institute; will you open it (e.g. using proxy)?	1	2	3	4	5

51.	By rule, you are not allowed to make a page about your institute on social media. Would you bypass the policy by making an unofficial one?	1	2	3	4	5
52.	You are always suggested to change your default password (email, LMS, CMS). Do you follow this practice?	1	2	3	4	5
	Peer Pressure	Never	Rarely	Sometimes	Often	Always
53.	Your friend saved the password on his system. Will you do the same practice?	1	2	3	4	5
54.	Your friends have a group on social media and they posted something negative about the institute. Will you comment or share the post?	1	2	3	4	5
55.	You and your friend received an email from a known/unknown sender. You don't want to open it but your friend did. Will you open it?	1	2	3	4	5

National University of Science and Technology,
H-12, Islamabad, Pakistan.

Declaration

Dear Respondents,

I, student of NUST studying the behavioral and environmental factors effects on students' Information Security Awareness. I assure you that, strictly following the research ethics, your replies will be kept strictly confidential and the data acquired will only be used for academic research purposes. This information will not be disclosed to anyone and the data will be summarized on a general basis only.

SECTION A: Demographic Data

Gender:	☐ Male	☑ Female		
Age:	☐ (18 or Under)			
	☑ (19 – 24)			
	☐ (25 – 31)			
	☐ (32 – 38)			
	☐ (39 or Above)			
Institute:	☑ SEECS	☐ MCS	☐ EME	☐ IGIS
Degree:	☑ Bachelors	☐ Masters		
Discipline: (e.g. BEE)	BESE	**Semester:**	7th	

SECTION B: Survey

The following statements concern your perception about yourself in a variety of situations. Please encircle the appropriate box against each statement to indicate the extent to which you agree or disagree with the statement by using the following scale.

	I see myself as someone who...	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1.	Does a thorough job.	1	2	(3)	4	5
2.	Is communicative, talkative.	(1)	2	3	4	5
3.	Is sometimes somewhat rude to others.	1	2	3	(4)	5
4.	Is original, comes up with new ideas.	1	2	(3)	4	5
5.	Worries a lot.	1	2	3	(4)	5
6.	Has a forgiving nature.	1	2	3	4	(5)
7.	Tends to be lazy.	1	2	3	(4)	5
8.	Is outgoing, sociable.	(1)	2	3	4	5
9.	Values artistic experiences.	1	2	3	(4)	5
10.	Gets nervous easily.	1	2	3	(4)	5
11.	Does things effectively and efficiently.	1	2	3	(4)	5
12.	Is reserved.	1	2	3	(4)	5
13.	Is considerate and kind to others.	1	2	3	4	(5)
14.	Has an active imagination.	1	2	(3)	4	5
15.	Is relaxed, handles stress well.	1	2	(3)	4	5
	Password Management					
16.	It's acceptable to use my social media passwords on my other accounts.	1	2	3	(4)	5
17.	It's safe to use the same password for social media and other accounts.	1	(2)	3	4	5

2

18.	I use a different password for my social media and other accounts.	1	2	(3)	4	5
19.	It's acceptable to share my passwords with friends.	1	2	3	(4)	5
20.	It's a bad idea to share my passwords, even if a friend asks for it.	1	(2)	3	4	5
21.	I share my passwords with friends.	1	2	3	(4)	5
22.	A mixture of letters, numbers and symbols is necessary for passwords.	1	2	3	(4)	5
23.	It's safe to have a password with just letters.	1	2	(3)	4	5
24.	I use a combination of letters, numbers and symbols in my passwords.	1	2	3	(4)	5
	Email Use					
25.	It's acceptable to click on any links in emails from people I know.	1	2	3	(4)	5
26.	It's always safe to click on links in emails from people I know.	1	2	(3)	4	5
27.	I don't always click on links in emails just because they come from someone I know.	1	(2)	3	4	5
28.	It's acceptable to click on a link in an email from an unknown sender.	1	(2)	3	4	5
29.	Nothing bad can happen if I click on a link in an email from an unknown sender.	1	(2)	3	4	5
30.	If an email from an unknown sender looks interesting, I click on a link within it.	1	2	3	(4)	5
31.	It's acceptable to open email attachments from unknown senders.	1	(2)	3	4	5
32.	It's risky to open an email attachment from an unknown sender.	1	2	3	4	(5)
33.	I don't open email attachments if the sender is unknown to me.	1	2	3	4	(5)
	Internet Use					
34.	It's acceptable to download any files onto my computer if they help me to do my job.	1	2	3	4	(5)
35.	It can be risky to download files on my computer.	1	2	(3)	4	5

3

36.	I download any files onto my computer that will help me get the job done.	1	2	3	(4)	5
37.	While I am at Institute, I shouldn't access certain websites.	1	2	(3)	4	5
38.	Just because I can access a website at Institute, doesn't mean that it's safe.	1	2	(3)	4	5
39.	When accessing the Internet at Institute, I visit any website that I want to.	1	2	3	(4)	5
40.	It's acceptable to enter any information on any website if it helps me do my job	1	2	(3)	4	5
41.	If it helps me to do my job, it doesn't matter what information I put on a website.	1	(2)	3	4	5
42.	I assess the safety of websites before entering information.	1	2	(3)	4	5
	Social Media Use					
43.	I will not be penalized for something I post on social media.	1	2	(3)	4	5
44.	It doesn't matter if I post things on social media that I wouldn't normally say in public.	1	2	3	(4)	5
45.	I don't post anything on social media before considering any negative consequences.	1	2	3	(4)	5
46.	I can post what I want about my Institute on social media.	1	2	(3)	4	5
47.	It's risky to post certain information about my Institute on social media.	1	2	3	(4)	5
48.	I post whatever I want about my Institute on social media.	1	(2)	3	4	5
	Secondary Source Influence					
49.	Based on what I have heard or seen on mass media (TV, radio, newspapers, internet), I am encouraged to follow information security best practices.	1	2	3	(4)	5
	Rule Following	Never	Rarely	Sometimes	Often	Always
50.	A website is blocked in your institute; will you open it (e.g. using proxy)?	1	2	(3)	4	5

51.	By rule, you are not allowed to make a page about your institute on social media. Would you bypass the policy by making an unofficial one?	(1)	2	3	4	5
52.	You are always suggested to change your default password (email, LMS, CMS). Do you follow this practice?	1	2	3	4	(5)
	Peer Pressure	Never	Rarely	Sometimes	Often	Always
53.	Your friend saved the password on his system. Will you do the same practice?	1	(2)	3	4	5
54.	Your friends have a group on social media and they posted something negative about the institute. Will you comment or share the post?	(1)	2	3	4	5
55.	You and your friend received an email from a known/unknown sender. You don't want to open it but your friend did. Will you open it?	1	2	(3)	4	5

Bibliography

Ahlan, A.R., Lubis, M. and Lubis, A.R., 2015. Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*, *72*, pp.361-373.

Al-Janabi, S. and Al-Shourbaji, I., 2016. A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(01), p.1650007.

Aloul, F., 2012. The need for effective information security awareness. *Journal of Advances in Information Technology*, *3*(3), pp.176-183.

Amankwa, E., Loock, M. and Kritzinger, E., 2014, December. A conceptual analysis of information security education, information security training and information security awareness definitions. In *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for* (pp. 248-252). IEEE.

Arachchilage, N.A.G. and Love, S., 2013. A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), pp.706-714.

Arachchilage, N.A.G. and Love, S., 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, pp.304-312.

Arpaci, I. and Baloğlu, M., 2016. The impact of cultural collectivism on knowledge sharing among information technology majoring undergraduates. *Computers in Human Behavior*, *56*, pp.65-71.

Atkinson, S., Furnell, S. and Phippen, A., 2009. Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security*, *2009*(7), pp.13-19.

Aurigemma, S. and Panko, R., 2012, January. A composite framework for behavioral compliance with information security policies. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 3248-3257). IEEE.

B. Kim, E., 2014. Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), pp.115-126.

Bada, M. and Sasse, A., 2014. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?.

Bardi, A. and Schwartz, S.H., 2003. Values and behavior: Strength and structure of relations. *Personality and social psychology bulletin*, 29(10), pp.1207-1220.

Barrick, M.R. and Mount, M.K., 1991. The big five personality dimensions and job performance: a meta-analysis. *Personnel psychology*, 44(1), pp.1-26.

Bauer, S., Bernroider, E.W. and Chudzikowski, K., 2017. Prevention is better than cure!

Brown, S.A. and Venkatesh, V., 2005. Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle. *MIS quarterly*, pp.399-426.

Byron, T., 2008. Safer children in a digital world: The report of the Byron Review: Be safe, be aware, have fun.

Chan, H. and Mubarak, S., 2012. Significance of information security awareness in the higher education sector. *International Journal of Computer Applications*, *60*(10).

Costa, P.T. and McCrae, R.R., 1992. NEO PI-R: Professional manual: Revised NEO PI-R and NEO-FFI. Florida: Psychological Assessment Resources.

Creswell, J. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.). Thousand Oaks, CA: Sage Publications, p. 217.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R., 2013.

Da Veiga, A. and Eloff, J.H., 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), pp.196-207.

Da Veiga, A. and Martins, N., 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, pp.162-176.

Da Veiga, A., 2016, July. A Cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In SAI Computing Conference (SAI), 2016 (pp. 1006-1015). IEEE.

Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68, pp.145-159.

Farooq, A., Isoaho, J., Virtanen, S. and Isoaho, J., 2015, August. Information security awareness in Educational Institution: An analysis of students' individual factors. In *Trustcom/BigDataSE/ISPA, 2015 IEEE* (Vol. 1, pp. 352-359). IEEE.

Flores, W.R., Antonsen, E. and Ekstedt, M., 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, pp.90-110.

Future directions for behavioral information security research. *Computers & Security*, *32*, pp.90-101.

Geert Hofstede, Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations. *Second Edition, Thousand Oaks CA: Sage Publications*, 2001

George, J.M. and Zhou, J., 2001. When openness to experience and conscientiousness are related to creative behavior: an interactional approach. *Journal of applied psychology*, 86(3), p.513.

Haeussinger, F. and Kranz, J., 2013. Information security awareness: Its antecedents and mediating effects on security compliant behavior.

Haeussinger, F., 2013. Understanding the Antecedents of Information Security Awareness-An Empirical Study.

Hahn, E., Gottschling, J. and Spinath, F.M., 2012. Short measurements of personality–Validity and reliability of the GSOEP Big Five Inventory (BFI-S). *Journal of Research in Personality*, 46(3), pp.355-359.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F. and Chen, J., 2016, November. Cultural and psychological factors in cyber-security. In Proceedings of the 18th *International Conference on Information Integration and Web-based Applications and Services* (pp. 318-324). ACM.

Halevishire, J., Warkentin, M. and Sharma, S., 2015. Personality, attitudes, and intentions: predicting initial adoption of information security behavior. *Computers & Security*, *49*, pp.177-191.

Hamid, H. and Zeki, A.M., 2014, December. Users' Awareness of and Perception on Information Security Issues: A Case Study of Kulliyyah of ICT Postgraduate Students. In *Advanced Computer Science Applications and Technologies (ACSAT), 2014 3rd International Conference on* (pp. 139-144). IEEE.

Hannah, D.R. and Robertson, K., 2015. Why and how do employees break and bend confidential information protection rules?. *Journal of Management Studies*, 52(3), pp.381-413.

Hanus, B. and Wu, Y.A., 2016. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), pp.2-16.

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

Hu, Q., Dinev, T., Hart, P. and Cooke, D., 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), pp.615-660.

Hui P, Buchegger S. Groupthink and Peer Pressure: Social Influence in Online Social Network Group. IEEE *Advances in Social Network Analysis and Mining* 2009

Ismailova, R. and Muhametjanova, G., 2016. Cyber crime risk awareness in Kyrgyz Republic. *Information Security Journal: A Global Perspective*, *25*(1-3), pp.32-38.

Jeske, D. and van Schaik, P., 2017. Familiarity with Internet threats: Beyond awareness. *Computers & Security*, *66*, pp.129-141.

John, O.P. and Srivastava, S., 1999. The Big Five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of personality: Theory and research*, 2(1999), pp.102-138.

Johnston, A. and Warkentin, M., 2012. The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. *End-User Computing, Development, and Software Engineering: New Challenges: New Challenges*, p.312.

Johnston, A.C. and Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, pp.549-566.

Karjalainen, M., Siponen, M.T., Puhakainen, P. and Sarker, S., 2013. One Size Does Not Fit All: Different Cultures Require Different Information Systems Security Interventions. In *PACIS* (p. 98).

Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J. and Linkman, S., 2009. Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, *51*(1), pp.7-15.

Komarraju, M. and Karau, S.J., 2005. The relationship between the big five personality traits and academic motivation. *Personality and individual differences*, 39(3), pp.557-567.

Kortjan, N. and Von Solms, R., 2014. A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, *52*(1), pp.29-41.

Kothari, C.R., 2004. *Research methodology: Methods and techniques*. New Age International.
Kritzinger, E., 2016. Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal*, *28*(1), pp.1-17.

Kruger, H.A. and Kearney, W.D., 2006. A prototype for assessing information security awareness. *Computers & Security*, 25(4), pp.289-296.

Kruger, H.A., Flowerday, S., Drevin, L. and Steyn, T., 2011, August. An assessment of the role of cultural factors in information security awareness. In *Information Security South Africa (ISSA), 2011* (pp. 1-7). IEEE.

Laudon, C.K., & Laudon, P.J., 2010. Management information systems. New Jersey: Prentice Hall.

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B., 2013, January. Employees' information security awareness and behavior: A literature review. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 2978-2987). IEEE.

Manke, S. and Winkler, I., 2012. The habits of highly successful security awareness programs: A cross-company comparison. Technical report, Secure Mentem, 2012. http://www. securementem. com/wp-content/uploads/2013/07/Habits_white_paper. pdf.

Marks, A. and Rezgui, Y., 2009, September. A comparative study of information security awareness in higher education based on the concept of design theorizing. In *Management and Service Science, 2009. MASS'09. International Conference on* (pp. 1-7). IEEE.

Martins, A. and Elofe, J., 2002. Information security culture. In Security in the information society (pp. 203-214). Springer, Boston, MA.

McBride, M., Carter, L. and Warkentin, M., 2012. The Role of Situational Factors and Personality on Cybersecurity Policy Violation.

McBride, M., Carter, L. and Warkentin, M., 2012. Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions*.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M., 2017. Individual differences and information security awareness. *Computers in Human Behavior, 69*, pp.151-156.

McCrae, R.R. and John, O.P., 1992. An introduction to the five-factor model and its applications. *Journal of personality, 60*(2), pp.175-215.

Mejias, R.J., 2012, January. An integrative model of information security awareness for assessing information systems security risk. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 3258-3267). IEEE.

Muhirwe, J. and White, N., 2016. CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS. *Issues in Information Systems, 17*(2).

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and 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), pp.126-139.

Ng, B.Y. and Rahim, M., 2005. A socio-behavioral study of home computer users' intention to practice security. *PACIS* 2005 Proceedings, p.20.

Ngoqo, B. and Flowerday, S., 2014. Linking student information security awareness and behavioural intent. In *HAISA* (pp. 162-173).

O. Lundy and A. Cowling, Strategic Human Resource Management, London: Routledge, 1996.
Öğütçü, G., Testik, Ö.M. and Chouseinoglou, O., 2016. Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, pp.83-93.

Ormond, D., Warkentin, M., Johnston, A.C. and Thompson, S.C., 2016. Perceived deception: Evaluating source credibility and self-efficacy. *Journal of Information Privacy and Security*, *12*(4), pp.197-217.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T., 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, pp.40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C., 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security*, *42*, pp.165-176.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. and Calic, D., 2015, August. Factors that influence information security Behavior: An australian web-based study. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 231-241). Springer, Cham.

Puhakainen, P. and Ahonen, R., 2006. Design theory for information security awareness, Faculty of Science, Department of Information Processing Science, University of Oulu, Finland, 2006.

Quinn, R.E., 1988. Beyond rational management: Mastering the paradoxes and competing demands of high performance. Jossey-Bass.

Rahim, N.H.A., Hamid, S., Mat Kiah, M.L., Shamshirband, S. and Furnell, S., 2015. A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), pp.606-622.

Ramalingam, R., Khan, S. and Mohammed, S., 2016. The need for effective information security awareness practices in Oman higher educational institutions. *arXiv preprint arXiv:1602.06510*.

Russell, J.D., Weems, C.F., Ahmed, I. and Richard III, G.G., 2017. Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security Technology*, pp.1-12.

Safa, N.S., Von Solms, R. and Furnell, S., 2016. Information security policy compliance model in organizations. *Computers & Security*, 56, pp.70-82.

Schein, E.H., 2009. The corporate culture survival guide (Vol. 158). John Wiley & Sons.

Shropshire, J., Warkentin, M., Johnston, A. and Schmidt, M., 2006. Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*, p.415.

Shropshire, J., Warkentin, M. and Sharma, S., 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, pp.177-191.

Silfver, M., Helkama, K., Lönnqvist, J.E. and Verkasalo, M., 2008. The relation between value priorities and proneness to guilt, shame, and empathy. Motivation and Emotion, 32(2), pp.69-80.

Siponen, M. and Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, pp.487-502.

Siponen, M., Mahmood, M.A. and Pahnila, S., 2009. Technical opinion Are employees putting your company at risk by not following information security policies?. *Communications of the ACM*, 52(12), pp.145-147.

Srisawang, S., Thongmak, M. and Ngarmyarn, A., 2015. Factors Affecting Computer Crime Protection Behavior. In *PACIS* (p. 31).

Stanciu, V. and Tinca, A., 2016. Students' awareness on information security between own perception and reality–an empirical study. *Journal of Accounting and Management Information Systems*, *15*(1), pp.112-130.

Stewart, G. and Lacey, D., 2012. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20(1), pp.29-38.

Straub, D., Loch, K., Evaristo, R., Karahanna, E. and Srite, M., 2002. Toward a theory-based measurement of culture. *Human factors in information systems*, *10*(1), pp.61-65.

Tan, M. and Sagala Aguilar, K., 2012. An investigation of students' perception of Bluetooth security. *Information Management & Computer Security*, *20*(5), pp.364-381.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E., 2015. Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), pp.38-58.

Uebelacker, S. and Quiel, S., 2014, July. The social engineering personality framework. In *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on* (pp. 24-30). IEEE.

van Muijen, J.J., 1999. Organizational culture: The focus questionnaire. *European Journal of Work and Organizational Psychology*, 8(4), pp.551-568.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. and Kusev, P., 2017. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*.

Vance, A., Anderson, B.B., Kirwan, C.B. and Eargle, D., 2014. Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems*, *15*(10), p.679.

Vance, A., Siponen, M. and Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3), pp.190-198.

Walaza, M., Loock, M. and Kritzinger, E., 2015, November. A pragmatic approach towards the integration of ICT security awareness into the South African education system. In *Information Security and Cyber Forensics (InfoSec), 2015 Second International Conference on* (pp. 35-40). IEEE.

Warkentin, M., Johnston, A.C., Shropshire, J. and Barnett, W.D., 2016. Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, *92*, pp.25-35.

Warkentin, M., Straub, D. and Malimage, K., 2012, June. Featured talk: Measuring secure behavior: A research commentary. In *Annual Symposium of Information Assurance & Secure Knowledge Management, Albany, NY*.

Webb, J.W., Ireland, R.D. and Ketchen, D.J., 2014. Toward a greater understanding of entrepreneurship and strategy in the informal economy. *Strategic Entrepreneurship Journal*, 8(1), pp.1-15.