An Empirical Analysis of the Information Security Culture Key Factors Framework

Alaa Tolah[1,2], Steven M. Furnell[1,3,5]and Maria Papadaki[1,4]

[1] University of Plymouth, Plymouth, United Kingdom

[2] Saudi Electronic University, Riyadh, Saudi Arabia

[3] University of Nottingham, Nottingham, United Kingdom

[4] University of Derby, Derby, United Kingdom

[4]Nelson Mandela University, Gqeberha, South Africa

Abstract:

Information security is a challenge facing organisations, as security breaches pose a serious threat to sensitive information. Organisations face security risks in relation to their information assets, which may also stem from their own employees. Organisations need to focus on employee behaviour to limit security failures, as if they wish to establish effective security culture with employees acting as a natural safeguard for information assets. This study was conducted to respond to a need for more empirical studies that focus on a development of security culture to provide a comprehensive framework. The Information Security Culture and Key Factors Framework has been developed, incorporating two types of factors: those that *influence* security culture and those that *reflect* it. This paper validates the applicability of the framework and tests related hypotheses through an empirical study. An exploratory survey was conducted, and 266 valid responses were obtained. Phase two of the study demonstrates the framework levels of validity and reliability through the use of factor analysis. Different hypothetical correlations were analysed through the use of structural equation modelling, with indirect exploratory effect of the moderators achieved through a multi-group analysis. The findings show that the framework has validity and achieved an acceptable fit with the data. This study fills an important gap in the significant relationship between personality traits and security culture. It also contributes to the improvement of information security management through the introduction of a comprehensive framework in practice, which functions in the establishment of security culture. The factors are vital in justifying security culture acceptance, and the framework provides an important tool that can be used to assess and improve an organisational security culture.

Keywords: Culture Framework, Information Security Culture, Human Factors, Employee Behaviour, Quantitively study.

1. Introduction

The growth of the technological environment has created challenges to information security and increased the potential for security breaches. Several studies have indicated that information security can no longer be achieved by technological issue alone but also is associated with people who actually operate these systems (Connolly et al. 2017; Mahfuth 2019). The interactions between human and information security have increased the possibility of security risks. It has been stated that the human dimension within the advancement of information security produces the weakest link in its development (Alhogail 2016; Connolly et al. 2017). 44% of organisations suffer security breaches by insiders (PwC 2013). An understanding of human factors is required to determine the reason behind unacceptable behaviour and make information security effective. Due to increasing number of security breaches caused by employee's behaviour, scholars and experts recommended to establish a security culture in guiding the security behaviour in organisations. The progression of security culture is vital to increase the levels of effectiveness in information security management (Walton 2015). A positive security culture contributes to support in guiding employees to follow security policies, which lowers the potential risk of harmful information interaction by employees, as they develop knowledge and advance their skills correctly, and behave securely in their working environments (National Cyber Secuirty Center 2017). The culture that promotes secure human behaviour through knowledge, values, and assumptions is better than regulations that merely mandate employees' behaviour (Alhogail 2016). Various studies suggest that security culture can lead employees to act as a "human firewall" (Alhogail 2016); where acting correctly is commonplace (Schlienger and Teufel 2003). As a result, organisations are required to use understandable guidelines to develop a culture of security awareness, which utilises various approaches to improve comprehension (Alhogail 2016; National Cyber Secuirty Center 2017).

A number of studies related to security culture have been used, ranging from understanding of security culture to the development and validation of security culture models and assessments (Nasir et al. 2019; Sas et al. 2020). However, few studies have developed and an empirically tested model, which comprehensively improves organisational security culture. This paper extends the Information Security Culture and Key Factors Framework (ISCFF) previously proposed by (Tolah et al. 2017; 2019), which facilitates an understanding of security culture and its elements and in is summarised in Section 2.

This study adopted the pragmatic approach with mixed methods of data collection. The first phase was a qualitative design to acquire sufficient information regarding security culture and signify the importance of factors in ISCFF from thirteen security specialists in organisations (Tolah et al. 2019). These findings confirmed the importance of identified factors, and this study extends the work to develop a statistical framework that identifies the correlations between factors. The study adopts a quantitative design as a second phase to evaluate the framework's effectiveness through an explanation of organisational security culture. Also, as this study relied on prior literature and semi-structured

interview to develop an initial ISCFF, it was considered using an exploratory survey to validate a framework and develop an understanding of the relationship between factors. The exploratory study assists in increasing the level of familiarity with the researched phenomenon of interest, which focuses on taking the most important parts and determining the most beneficial way of measuring them (Recker et al. 2008). Due to the lack of reliability and validity in the security culture measurements, as the literature shows, the exploratory survey has adopted in this study to validate the importance of each factor proposed in the framework. Also, the exploratory survey will enhance the testing of data validity and reliability (Alnatheer et al. 2012). The main aims of a survey to test the framework's validity and reliability, validate factors in ISCFF and test hypotheses.

Therefore, this paper presents the findings from a survey with 266 valid responses to provide the framework levels of validity and reliability. The paper initially provides a review of related work for security culture models in addition to a detailed review of ISCFF and hypothesis development. Subsequently, the study method is described with the analytical approaches used to interpret the results. The paper concludes by outlining the study implications and future research.

2. Establishing the Research Framework

Instilling an effective culture is vital to create adequate levels of information security. Various studies provide an overview that focuses on security culture (Alhogail 2016; Nasir et al. 2019; Sas et al. 2019). Their literature analyses concluded that most investigated issues in security culture relate to the conceptualisation of culture to identify concepts and factors that affect security culture, the creation of security culture, or an assessment of security culture to measure whether it is an adequate level. Many studies provide various approaches and models that highlight security culture's importance, promote its benefits and provide guidelines to develop a security culture. The literature analysis showed that most studies demonstrated various essential factors that may shape or change security culture (Nasir et al. 2019). A comprehensive review of security culture was conducted in prior work (Tolah et al. 2017) to gain an overview of the current available models, which focused on studies that assess security culture and presented an essential knowledge with regards to factors that help in developing security culture. Fourteen research perspectives relate to the creation of security culture and six studies incorporate an assessment of security culture. The security culture is a product of various factors, such as security policy and security training that affect the individual's behaviour in organisations (Tolah et al. 2017). These studies have developed comprehensive security culture models and contributed to how organisations potentially create and maintain acceptable security culture levels.

However, few studies have used the same framework to create and assess security culture. Studies by (Alhogail 2016) and (DaVeiga and Eloff 2010) provide an approach that utilises the same framework to create and assess security culture, which both provide statistically sound assessment instruments to

perform security culture assessment. There is no mutual agreement on factors that have to be considered for developing a security culture. There are limited studies that have identified the factors that reflect a security culture (Nasir et al. 2019). Few studies have provided reliable and valid security culture assessment instruments. Schlienger and Teufel (2003) designed a questionnaire to detail how proper rules impact upon employees' security behaviour, while Da Veiga and Eloff (2010) designed a security culture assessment tool. Also, there is minimal coverage of other influential factors, such as individual difference variables and job satisfaction. The positive impacts of these factors on workplace behaviours had proven by studies from (Greene and D'Arcy 2010; McCormac et al. 2017) Few studies used a mixed method and validate their models using different validation techniques such as a structural equation modelling. The literature review illustrated that there is a need for more investigation in the area to provide comprehensive frameworks and the best practices of security culture cultivation and assessment.

In order to overcome the lack of comprehensive frameworks, the author has proposed a comprehensive ISCFF in (Tolah et al. 2017). The development of ISCFF is based on Alnatheer's model and a review of academic literature in the security culture. ISCFF initially helps researchers and practitioners in comprehending whether the level of security culture enhances the security of information assets and assesses the relationship between factors. In the ISCFF, the security culture comprises several factors, as the components are structured into: factors that influence security culture (top management, security policy, security education and training, security risk assessment and analysis, and ethical conduct); factors that reflect security culture (security awareness, security ownership and security compliance); and factors of organisational behaviour that contribute to workplace behaviours and influence the security culture (personality traits and job satisfaction) (see Figure 1). These factors appear to be the most influential factors and are considered as part of security culture's conceptualisation. By understanding the influential factors or reflection factors, it is possible to aid in directing the interaction of humans with information security. These factors provide management with a means to implement adequate security management approaches that include the guidance provision and implementation of security culture.

Figure 1. Information Security Culture and Key Factors Framework (Tolah et al. 2017, 2019)

Seven hypotheses were developed with respect to the discussed theoretical background and study objectives. The developed hypothesises (H1 to H7a-e) explain the relationship between factors based on the qualitative findings in (Tolah et al. 2019) incorporated with the literature review analysis to be tested through the survey phase. The next subsections deliberate on these factors along with hypotheses.

2.1. Influential factors

This category includes five sub-factors. The support from top management has shown to be one of the important factors that leads to the information security success in organisations (Knapp et al. 2006; Barton et al. 2016). Top Management refers to a degree of how senior leadership understands the importance of information security function and is involved in the security activities to create a strong security culture (Martins and Da Veiga 2015). The interview findings supported this concept in the development of information security in various companies. Top management figures are able to ensure that staff members remain accountable for each action and decision in relation to security. As a result, the top management influences the development of security culture. This would not be developed without implementing consistently positive encouragement and involvement from these figures (Masrek et al. 2018). Thus, it is hypothesised:

H1: Top management support has a positive influence on the effectiveness of security culture.

Security policy was considered one of important factor in the cultivation of security culture. Security policy is a written document that specifies the organisation's strategies and requirements of the security approach that guide both the management and employees' behaviour (Martins and Da Veiga 2015). The findings showed that a clear and effective security policy has a tendency to promote security-cautious behaviour in organisations. Combining the findings from the literature reviews and interview data, it has been suggested that a security policy must be enforced and be a top priority in organisations. It will encourage security compliance, through security awareness and establish an acceptable level of security culture (Alhogail 2016). It is hypothesised:

H2: Security policy has a positive influence on the effectiveness of security culture.

Security education and training is the most important factor that influences the effectiveness of security culture. Security education and training is a learning process that provides general knowledge of a certain subject related to the security environment and the required security skills for employees to perform the security procedures (Martins and Da Veiga 2015). The qualitative finding supports the previous studies, which show that a security culture is unattainable without the sufficient level of security training for all employees in organisations (DaVeiga and Eloff 2010). It is important to conduct periodic security training sessions to develop a culture of information security. This helps to reduce risks to information assets and improve the awareness of employees which, in turn, has a tendency to encourage security compliant behaviour (DaVeiga and Eloff 2010). It is hypothesised:

H3: Security education and training has a positive influence on the effectiveness of security culture.

The importance of considering a security risk assessment and analysis has been shown in the literature review and interview findings. Risk analysis and assessment defined as when countermeasures are adequate to decrease the probability of loss or the effect of loss to an acceptable level. Security risk analysis and assessment help the organisation and its employees to be capable of understanding potential damage to security. It helps to increase awareness and knowledge, which improves the level of security culture (Alnatheer 2012). It is hypothesised:

H4: Security risk analysis and assessment has a positive influence on the effectiveness of security culture.

Ethical conduct is vital factor that affect the security culture cultivation. It serves as a guideline that clarifies and defines actions deemed to be ethical. Ethical conduct enables employees to understand their own responsibilities. As the employee adheres to policies, it reduces potential security behaviour risks (Alnatheer 2012). Ethical conduct policies strongly affect a security culture. When failed to be

applied, the security nature in the organisation decreases. Thus, this needs to be developed in order to have an effective security culture. It is hypothesised:

H5: Ethical conduct has a positive influence on the effectiveness of security culture.

2.2. Organisational behaviour factors

This category has two factors: job satisfaction and personality traits. The job satisfaction plays an important role in employees' behaviour and attitudes towards information security (Farokhi et al. 2016). Job satisfaction helps to determine how employees may adapt to situational factors, such as remaining committed and not opting for easier options, which could prove detrimental to the organisation (Greene and D'Arcy 2010). The review of the literature and interview findings indicated that higher job satisfaction motivates employees to comply with security policies in organisations. So, the organisation will have employees with the right attitudes and willingness to fulfil job responsibilities and commit to a security culture. Also, there is a strong correlation between the security culture, security compliance and the behavioural role of employees (Greene and D'Arcy 2010). It is hypothesised:

H6: Job satisfaction has a positive influence on the effectiveness of security culture.

This study examined whether personality traits contribute positively or negatively to the level of security culture in organisations. The literature review demonstrated that individual personality traits affect security behaviour. The personality traits potentially help in improving individuals' awareness of security and information asset security in organisations (McCormac et al. 2017). Personality traits describe the personality factors, their potential factors and helps to understand the variability between individuals to understand the underlying psychological mechanisms which might affect user behaviour toward information security (McCormac et al. 2017). The most commonly used taxonomy in research into peoples' personalities is the five-factor model (FFM) and has become widely accepted in this form of research, as it has good validity, which was shown by various empirical studies (Goldberg 1993). The aim of the model is to divide human personality into five factors that enable the theoretical conceptualisation of personalities: extroversion, agreeableness, openness, neuroticism, and conscientiousness (John and Srivastava 1999).

It had been indicated that agreeableness is a positive factor in relation to work (Barrick et al. 2001). It involves notable interpersonal interaction, particularly in regard to job tasks through helping others and cooperation. People who have a personality trait of agreeableness are commonly courteous, trustworthy, cooperative, compliant, and are often tolerant and forgiving (Barrick et al. 2001). An individual's agreeableness has been deemed to have a positive connection with increased levels of organisational safety. The correlation between agreeableness and information security has been analysed to stem from an employee's attitude towards information security when this involves

collaboration with others. Pattinson et al. (2015) study provided an evaluation of non-malicious computer-based behaviour. It was determined that when an employee presents naivety in relation to accidents that they are not at such a high risk when they are more agreeable. Individuals who have high agreeableness scores normally become more concerned with security issues, as they commonly think about others' opinions of them (Shropshire et al. 2015). Also, agreeableness was shown to have greater effects on policy in regard to user compliance (Shropshire et al. 2006). It can be deduced that agreeable employees are influential upon positive security cultures.

H7a: Agreeableness has a positive influence on the effectiveness of security culture.

Conscientiousness is one of the most relevant personality traits to information security behaviour (Shropshire et al. 2006). Conscientiousness is a trait associated with planning and persistent behaviour. When people are conscientious, they are hard-working, and as normally focus on achievement are motivated, dependable, responsible and ambitious (Barrick et al. 2001). Shropshire et al. (2006) noted that conscientiousness has the highest impact upon policy with user compliance. Compliance with security policy was more likely with conscientious individuals. Similarly, McCormac et al. (2017) determined that conscientious individuals are significantly more security aware. The higher levels of conscientiousness commonly resulting in more care as security requirements are considered more, with a focus on improving information security and the overall security culture. It is hypothesised:

H7b: Conscientious has a positive influence on the effectiveness of security culture.

It have been stated that openness is fundamental to a person's personality (McCrae and John 1992). Openness enables the ability to explore various forms of information that attracts different situations. Employees who are open to experience, are generally inventive, creative, open-minded, more intellectual and imaginative (Barrick et al. 2001). McBride et al. (2012) developed comprehension levels for personality traits which comprise behavioural patterns and impact upon employees' intentions to adhere to the security policies. Their study results showed that security policy compliance is more likely with employees who are more open. Employees who present higher levels of openness to new experiences are normally better at problem solving. They have better critical thinking skills, that increase security awareness and security compliance. It is hypothesised:

H7c: Openness has a positive influence on the effectiveness of security culture.

An extraverted personality has been shown to result in improved task performance through interpersonal interactions (Mount et al. 2005). Extraverts normally aim to establish a favourable social status and then maintain it (Mount et al. 2005). When an individual is extroverted, they generally exhibit

positive emotionality, ambition, energy and dominance in various situations and settings. A study of (Bansal 2011) analysed the relation of FFM, focusing on website security and privacy and showed that extraversion has a positive effect on security concerns. The extroverted employees exercise a proactive external nature with internal information procurement in relation to security breaches, and legislation and communication through. This helps to increase their awareness and performance levels. Employee who are highly extraverted are more likely to have a positive attitude towards a security culture.

H7d: Extraversion has a positive influence on the effectiveness of security culture.

Emotional stability (the counterpart of neuroticism) has been shown as a valid predictor that improved job performance (Barrick et al. 2001). Emotional stability is the opposite of neuroticism. The individual becomes less anxious, pessimistic, hostile, and less personal insecurity. Neurotic individuals demonstrate levels of worry, sadness, low-confidence, depression, anger, and feelings of insecurity (Barrick et al. 2001). The study of (McBride et al. 2012) increased the understanding of personality traits that comprise behavioural patterns. The individual personality traits are impactful on employees' intentions that adhere to security policies, with neuroticism often leading to security policy violations. The study of (McCormac et al. 2017) analysed the correlations between certain personality differences through personality tests and security awareness measurements. It was consequently determined that emotional stability is noticeably effectual upon employees' security awareness. It is hypothesised:

H7e: Neuroticism has a negative influence on the effectiveness of security culture.

Table 1 summarises the main hypothesis to be tested through the survey phase. The first three of these (H1, H2, H3) have been proven to have a positive impact on the security culture in previous studies, such as (Knapp et al. 2006; Martins and Da Veiga 2015; Nasir et al. 2019).

Table 1. Research Hypothesis

	Hypothesis
H1	Top management support has a positive influence on the effectiveness of security culture.
H2	Security policy has a positive influence on the effectiveness of security culture.
H3	Security education and training has a positive influence on the effectiveness of security culture.
H4	Security risk analysis and assessment has a positive influence on the effectiveness of security culture.
H5	Ethical conduct has a positive influence on the effectiveness of security culture.
H6	Job satisfaction has a positive influence on the effectiveness of security culture.

H7a	Agreeableness has a positive influence on the effectiveness of security culture.
H7b	Conscientious has a positive influence on the effectiveness of security culture.
H7c	Openness has a positive influence on the effectiveness of security culture.
H7d	Extraversion has a positive influence on the effectiveness of security culture.
H7e	Neuroticism has a negative influence on the effectiveness of security culture.

2.3. Security culture factors

This study determined that security culture is perceived as a second-order factor, which involve security awareness, security ownership and security compliance. The interviews findings from (Tolah et al. 2019) provided confirmation of these three factors that reflect security culture. Security awareness is an imperative factor of security culture. Security awareness defined as when users understand the potential of information security-related issues and become aware of their security mission (DaVeiga and Eloff 2010). Awareness by employees is one of the main challenges the organisations face in achieving an adequate level of security. Both security education programs and the security policy have tendency to encourage compliant behaviour by increasing security awareness of employees. When employees are aware of security policies, compliance with the security policy is achieved; thus, there is a development in security culture (Schlienger and Teufel 2003). As a result, security awareness is the main factor that results in greater levels of compliance and advance security culture (Wiley et al. 2020).

It has been shown that security ownership is vital in the security culture cultivation. Security ownership refers to how employees view their responsibilities in security and their willingness to act in a supportive manner to enhance their own security performance (Alnatheer 2012). When the responsibilities are understood, as well as the necessity of protecting information, employees are able to understand the security risks that can be a result of their own actions. As a result, this increases the security awareness, and the security policy compliance and thus leads to the establishment of security culture (Sas et al. 2019). The literature review and qualitative results illustrated the importance to improve the security compliance towards the creation of security culture. Security compliance refers to how the employees' behaviour complies with the security policy to reduce the security breaches that caused by employees' misbehaviour (DaVeiga and Eloff 2010). It has been demonstrated that security compliance is necessary to the management of information security, and to the creation of security culture (Schlienger and Teufel 2003).

3. Methodology

This study used a pragmatic approach with mixed methods of data collection. The first phase was a qualitative design to signify the importance of the identified factors in ISCFF. Semi-structured interviews with thirteen IT/security specialist were conducted in an exploratory manner, as they presented their opinions and relevant feedback regarding the factors and understanding of framework. A more detailed description of the qualitative study can be found in (Tolah et al. 2019). The second phase, which involved quantitative data via an exploratory survey, was conducted to validate the ISCFF and test hypotheses. Different analysis techniques were also conducted, particularly Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), and Structural Equation Modelling (SEM), which were based on the questionnaire's obtained data.

3.1. Measurement of Variables

The survey is divided into four parts, firstly the demographics information. It collects information regarding the type and size of an organisation, the organisation industry, gender, age, country, employees' qualification levels in the field of IT, experience levels and job level. Second, knowledge section that aims to evaluate the security knowledge and awareness levels of employees. It includes nineteen questions that focused on the framework's scope, which adopted from prior studies, (Alhogail 2016; Knapp et al. 2006; DaVeiga 2018). The questions' scale was "Yes/No" or "do not know".

The third part was security culture practices to assess employees' perspectives and perception toward the framework factors. A comprehensive literature review and qualitative findings were combined, together with expert reviews in order to determine the specific constructs and their related survey items that influence and constitute the security culture (Alhogail 2016; Tolah et al. 2017; DaVeiga 2018). The survey dimensions were identified to measure ten factors: top management (TM); security policy (SP); security education and training (SET); security risk analysis and assessment (RA); ethical conduct (EC); job satisfaction (JS); personality traits (PT); security awareness (SA); security ownership (SO); and security compliance (SC). The components of the framework were divided into several representative statements. Then, statements were grouped together as clusters that represented the dimensions' different elements and their connections. This section includes thirty-four statements, all constructed as closed questions. The majority of statements were adapted from previously validated instruments from these studies (Spector 1997; Knapp et al. 2006; Alnatheer 2012; Alhogail 2016; DaVeiga 2018). From these adapted scales, it was possible to increase the framework's level of reliability and validity. Other statements were taken from the interview responses and the feedback from experts. A full description of constructs with the number of measuring items, and their adoption source as presented in Appendix A.

The last part was the personality test relates to big five factor model dimensions (FFM). It aims to present a better understanding of human personality traits and identify organisational predictive values for security behaviour. This part contains forty-four items that cover five dimensions: agreeableness, conscientiousness, extraversion, neuroticism, openness. All these dimensions were adapted from (Shropshire et al. 2006; Goldberg 1993). All survey items were measured based on five-point scales ranging from "strongly disagree" to "strongly agree," except for knowledge part.

A pre-test was utilised using two methods to ensure the validity and reliability of survey. First, a draft of survey was sent via email to six professional experienced experts in the field of security culture implementation in order to review and judge whether the items measured the presented theoretical construct. Reponses were requested on clarity, relevance, and the quality of items. Based on the reviewer feedbacks, certain changes were made to the survey to increase readability. Various items were also changed, and items included following certain critique. Then, a pilot study conducted with eleven participants from educational institute in the United Kingdom were able to complete the survey without a need for explanation of wording or clarification of ambiguity. Certain statements that were unclear were reviewed and the comments from the participants in regard to the wording and structure were used to improve the survey. The final survey was also revised and developed. All constructs are considered reflective. The measurement of security culture (SC) was taken as a second-order construct composed of first-order constructs: security awareness, security ownership and security compliance. All constructs and corresponding items in their final version can be found in Appendix A.

3.2. Sample and Data Collection

This study used a non-probability method because of the limitation of time and cost. Access to a target population is often difficult. The study adopted the convenience and snowball sampling (Saunders et al. 2009). These techniques helped to gain easy access to different participants. The target population selected for this study were individual employees who work in any type of organisation. The overall sample was developed by the number of participants, who met the participation criteria and were willing to participate in the study. The initial respondents were further encouraged to recruit more people from their companies to complete the survey. The initial target population was included a representative sample of American, British, and Saudi societies because this study interviewed employees from these societies in the first phase of data collection.

It is essential to send a survey to different organisations from a wide range of sectors and industries, which may require different levels of security. The ability to compare between industry/sectors helps to demonstrate particular security culture traits for each one, which can potentially result in different levels of investment in security awareness and relevant security training programmes (Roer and Pertic 2017). Nonetheless, access to appropriate organisations was difficult, as certain organisations are

restricted against discussing security management. However, the low number of responses, which could be due to time restrictions and limited access to different organisations, resulted in the survey also being posted online at https://www.callforparticipants.com. The final number of responses was 266 from a mix of three countries: Saudi Arabia, United Kingdom and United State of America and other countries such as Australia and South Africa, which covered private, public, and semi-public sectors, and included various industries such as education and health. The respondents worked in different operational, technical positions and departments, comprising operational staff, administrative, IT, security staff, and managers. However, the diversity of organisations' geographical locations would assist in advancing the understanding of security culture from varied backgrounds.

The cross-sectional survey was adopted in an exploratory manner to test the validity of the framework, validate the factors intended in ISCFF and test the hypothetical relationship between factors. Table 2 below summaries demographic characteristics.

Table 2. Demographic characteristics of a sample

Demographic Characteristics	**Options**	**No**	**%**	**Demographic Characteristics**	**Options**	**No**	**%**
Type of Organisation	Private	113	43	Country of Residence	SA	84	31.5
	Public	139	52		Other	73	27.4
	Semi-public	14	5		UK	89	33.4
					USA	20	7.5
Industry	Education	123	46.2	The qualification Levels in the field of IT	Yes	100	37.4
	Healthcare	28	10.6		No	166	62.4
	Other	109	42.9				
Organisation Size	Less than 250	84	32.2	Length of Employment	Less than 1	57	21.5
	250 – 1000	62	23.2		1 – 4 years	94	35.8
	More than 1000	120	45.1		5 – 10 years	67	25.2
					More than 10	48	18
Age	Under 25	51	20.1	Job Level	Senior Manager	25	9.6
	25-35	113	42.9		Middle Manager	55	20.9
	36-45	62	23.2		Depart Manager	35	13.4
	46-55	24	9.1		Security staff	11	4.3
	56 and above	16	6.3		Technological staff	34	13
Gender	Male	112	42.5		Operational staff	60	23.2
	Female	147	55.3		Other	46	17.3
	Prefer not to say	7	2.8				

Note: No: Number, SA: Saudi Arabia, UK: United Kingdom, USA: United State of America, Depart: Department

A self-reported online questionnaire was used to collect data that was administered via the web-based survey platform, Qualtrics.com. The data was collected between December 2018 and December 2019. A survey distributed via e-mail with an invitation to 600 organisations to fill in a survey online. These direct invitations detailed the study purpose and contained a link to the online survey. The cover letter described the study goals, the time requirement to complete, and advised that participation was completely voluntary, and all details would remain confidential. The survey was made available in English and Arabic. The typical time required to answer the survey was fifteen to twenty minutes, with the respondents able to answer the questions in their own time and convenience. The responses were monitored to ensure that statistically representative number of responses were achieved and ensure that

the demographical groups were evident. A total of 266 surveys were completed with valid responses, which were then collated and combined for analysis. Companies were a range of sizes and geographical locations, the United Kingdom, the United State of America, and Saudi Arabia. The respondents came from a mix of hierarchical levels in their organisations, as well as locations, backgrounds, levels of positions and age groups.

4. Analysis and Results

The survey data analysis was segmented into two stages: preliminary data analysis that presents the descriptive statistics; and partial least square structural equation modelling (PLS-SEM) to validate the ISCFF and determine the relevant factors that positively affect a security culture. PLS-SEM is appropriate for complex models (Lowry and Gaskin 2014) and has fewer restrictions in relation to data distribution and the sample size (Vinzi et al. 2016). The framework in Figure 1 was tested through two steps on a hierarchal basis. First, the measurement model was assessed to examine psychometric reliability and validity tests using Confirmatory Factor Analysis technique. Then, the structure model was assessed to determine the relationship between factors and the predictive validity of the model. The moderating impact of demographic information on the proposed relationships have assessed by a multiple group analysis (MGA) technique. This study used the bootstrap method for a total of 500 cases with 2000 samples in order to obtain the t-value. For these phases, established guidelines of (Hair et al. 2016) were followed.

Before performing PLS-SEM, an analysis of scale reliability was tested through an assessment of internal consistency (Cronbach's α) and construct validity were achieved through applying a factor analyses using first Exploratory Factor Analysis technique to inform a scale validity evaluation and group the multiple items from the same construct. Following this, Confirm Factor Analysis evaluated the measurement model to determine the reliability, discriminant validity and convergent validity of items and constructs. The data was quantitatively analysed using the Statistical Package for the Social Sciences (SPSS) software for descriptive analysis and EFA, and Smart PLS version 3.3.2 for the partial least square (PLS) modelling to analyse the data.

A pre-analysis of data was screened before the statistical analyses to addresses the levels of data accuracy. Data screening was conducted in SPSS software, that included an evaluation of missing data, multivariate normality, multivariate outliers and common method bias (CMB). It was determined that the data screen demonstrated no missing data, as the participants had completed the full survey. For testing data normality, skewness and kurtosis were performed. The results show normality in data as all the constructs have skewness and kurtosis values in the accepted range of (0.22 to 1.09 and -1.09 to 1.15), respectively (see below Table 3). This range is within the stated recommendation -2.00 to +2.00 (Hair et al. 2016). Mahalanobis Distance (D2) values were calculated for each case and no multivariate

outliers were found. All of the p values for the computed Mahalanobis D2 values exceeded 0.001, providing evidence that the variables included no multivariate outliers at 0.001 level of significance that would affect the data and be held for additional analysis. The Harman one factor test was conducted using EFA with extraction method of Principle Component Analysis (PCA) to assess CMB problem. The results indicated fourteen factors with eigenvalues above 1, with the first factor explaining a variance of 20.5%. This confirmed that there was no problem with the CMB, as the study's first factor does not explain a major variance and none of the factor was found apparent. The following subsections present the results for analysis.

4.1. Descriptive analysis

The ISCFF variables were measured through the use of descriptive statistics, including mean, standard error (SE) and standard deviation (SD). The mean values calculated from the whole sample. In order to obtain the complete mean level for all constructs, the components' items scores were shown through their average, which comprised: top management, security policy, security education and training, security risk analysis and assessment, ethical conduct, job satisfaction, personality traits that include (agreeableness, conscientiousness, extraversion, neuroticism, openness), security awareness, security ownership and security compliance that were calculated in order to create fourteen composite variables.. The mean values were shown to represent the variables' responses, and the mean values ranged between 1.65 and 3.30. This indicated a general tendency for the numerically coded responses to demonstrate a value that is between neither 'disagreeing' nor 'agreeing' with the individual items (score = 3) and merely 'agreeing' with the items (score = 2). SD had a range of 0.42 to 0.86 and SE had a range of 0.02 to 0.05 (see Table 3). For the entire variables, the SD and SE were at a relatively small level in comparison to the means levels. Thus, the mean value can be used as a representative score for the variables in the data sets.

Table 3. Framework Constructs Results Statistical Analysis Summary

Construct	Mean	SE	SD	Skewness	Kurtosis
Top Management	2.14	0.03	0.57	-0.17	-0.47
Security Policy	2.11	0.04	0.67	0.08	-0.38
Security Education and Training	2.21	0.03	0.61	-0.21	-0.39
Risk Analysis and Assessment	1.90	0.03	0.58	0.62	1.15
Ethical Conduct	1.66	0.04	0.67	1.09	0.99
Job Satisfaction	2.19	0.03	0.60	0.15	-0.17
Security Awareness	1.74	0.03	0.52	0.16	-0.47
Security Ownership	1.65	0.03	0.54	0.42	-0.47
Security Compliance	1.79	0.03	0.53	0.21	-0.41
Extraversion	2.25	0.02	0.42	-0.01	0.05
Agreeableness	1.97	0.02	0.47	0.66	0.93
Conscientiousness	1.91	0.02	0.47	0.80	0.71
Neuroticism	3.30	0.05	0.86	-0.22	-1.09
Openness	2.01	0.02	0.43	0.27	0.01

Notes: SE: Standard Error, SD: Standard Deviation

In the analysis of security knowledge statements, frequency distribution was used. The data demonstrates that the general awareness and knowledge levels among employees. The majority of respondents were well informed of security policies (80.6%). 66.9% of respondents stated that they were aware of their security responsibilities. 63.9% of respondents noted that they are aware of the code of ethics. 66.9% of respondents stated that their companies include a team that assessed information asset risk levels. These teams regularly provided updates related to security risks. 48.5% of respondents had never attended any security training session. An attention needs to pay to a security knowledge and particularly for targeted security training and awareness. The results showed a failure in the access to updates security policy material (38.7%) and security training programmes (49.6%), which can result in inadequate levels of security awareness and compliance.

4.2. Factor Analysis - Exploratory Factor Analysis

Exploratory Factor Analysis (EFA) was performed to inform a scale validity evaluation and examine the measurement items' structure that corresponded to the variables in the framework. EFA was used for the individual constructs, as this helped to present the relevant number of factor structures. The correlation matrix was investigated using Kaiser-Meyer-Olkin (KMO) test and Bartlett's test of sphericity. KMO value was 0.79 higher than the lowest acceptable level (0.60) (see Table 4). The Bartlett's test was significant at $p<0.001$, as this adhered to the initial assumptions for EFA (Bartlett 1954; Kaiser 1974). The results confirmed the factorability of EFA conducted for constructs.

Table 4. KMO and Bartlett's Test of Sphericity

		Bartlett's Test of Sphericity		
Construct	**KMO**	**Approx. Chi-square**	**df**	**Sig.**
ISCFF framework	0.790	11310.484	3103	0.000

PCA extraction with the orthogonal varimax rotation were used in the examination of correlation patterns of seventy-seven items. The correlation matrix factorability was investigated using Pearson's product-moment correlation coefficient. Fourteen factors were extracted based on Kaiser's criterion of eigenvalue >1 with a complete variance of 59.4%. The items shared above 0.50 communalities with their factors. Seventy-five items had a loading of at least to 0.50 with the primary factor, which indicated a practical significance and satisfied to the minimum factor loadings' criterion (Hair et al. 2016) (see Appendix B). Two items SET2 and JS3 were deleted, as there were low-loading and cross-loading levels with other factors. EFA provided evidence of quality measurement scales for factors with high levels of validity.

4.3. Measurement Model Assessment – Confirmatory Factor Analysis

The measurement model presents various sequenced relationships which depict the way that measured variables show a construct (reflective or formative) that is not directly measured (Hair et al. 2016). The measurement model used factor analysis in the assessment of observed variables and how they are loaded in their underlying construct (Hair et al. 2016). This approach began through the model's specifications and uses CFA in the reliability and validity assessment. In this study, the measurement model presents only reflective constructs. The validity and reliability assessment of a reflective measurement model includes: composite reliability (CR) that evaluates internal consistency reliability; individual indicator reliability; average variance extracted (AVE) to evaluate convergent validity; and discriminant validity (Hair et al. 2016). Regarding internal consistency reliability, Cronbach's α and CR were found in the acceptable range (see Table *5*). Cronbach's α value was higher than the requirement value of 0.50 (Hair et al. 2016). The CR value between 0.77 to 0.93; exceeded the threshold of 0.70 (Hair et al. 2016). The indicator reliability was assessed with factor loadings of items and should exhibit values above 0.70. Items with an outer loading between 0.50 and 0.70 can be kept in the model, while indicators of less than 0.50 need to be removed (Hair et al. 2016). All values in the accepted range between 0.51 and 0.89, except twelve items from the personality trait (PT) (particularly from agreeableness, conscientiousness, extraversion, openness, neuroticism) were removed due to their low level of loading (see Appendix C). The convergent validity tests establish the validity of the constructs. The AVE values were above 0.50, which indicates the sufficient average variance extracted by the items (see Table 5). Discriminant validity was assessed with Fornell and Larcker's criterion. Fornell and Larcker's criterion compares the square root of the AVE against the latent construct correlation. A latent variable is required to share more variance with the assigned indicators than in relation to different latent variables (Hair et al. 2016). The AVE's square root of each construct needs to be higher than the correlation values of a construct with other constructs, this study met the condition, as shown in Table 6. There are no inter-construct correlation values in excess of the AVE's square root of the AVE. All the criteria were met and provided support for the measure's reliability and validity, which allowed to test the hypotheses through structural model.

Table 5. Validity, Reliability and Collinearity

Construct	α value	CR	AVE	VIF
Top Management (TM)	0.68	0.80	0.50	1.80
Security Policy (SP)	0.79	0.86	0.62	1.95
Security Education & Training (SET)	0.55	0.77	0.53	1.78
Risk Analysis & Assessment (RA)	0.63	0.80	0.58	1.73
Ethical Conduct (EC)	0.86	0.91	0.78	1.76
Job Satisfaction (JS)	0.79	0.85	0.54	1.29
Agreeableness (Agr)	0.84	0.88	0.52	1.17
Conscientiousness (Con)	0.84	0.87	0.50	1.17
Extraversion (Ext)	0.86	0.89	0.58	1.05

Neuroticism (Neu)	0.91	0.93	0.72	1.02
Openness (Ope)	0.84	0.87	0.51	1.25
Security Awareness (SA)	0.66	0.81	0.59	-
Security Ownership (SO)	0.76	0.86	0.67	-
Security Compliance (SC)	0.63	0.79	0.57	-

Notes: α: Cronbach's α, CR: Composite Reliability, AVE: average variance extracted, VIF: Variance Inflation Factors

Table 6. Discriminant Validity-Fornell Larcker Criterion

	Agr	**Con**	**EC**	**Ext**	**JS**	**Neu**	**Ope**	**RA**	**SA**	**SC**	**SET**	**SO**	**SP**	**TM**
Agr	**0.72**													
Con	0.22	**0.71**												
EC	0.27	0.19	**0.88**											
Ext	0.02	0.08	0.17	**0.76**										
JS	0.11	0.10	0.25	0.06	**0.73**									
Neu	0.01	-0.10	-0.02	0.04	-0.04	**0.85**								
Ope	0.25	0.26	0.28	0.11	0.27	0.03	**0.71**							
RA	0.22	0.19	0.55	0.10	0.28	-0.05	0.23	**0.76**						
SA	0.28	0.18	0.50	0.15	0.32	-0.07	0.25	0.52	**0.77**					
SC	0.30	0.28	0.59	0.20	0.41	-0.09	0.34	0.60	0.57	**0.75**				
SET	0.20	0.25	0.51	0.06	0.29	-0.10	0.24	0.54	0.54	0.52	**0.73**			
SO	0.33	0.30	0.50	0.02	0.34	-0.11	0.31	0.53	0.55	0.63	0.48	**0.82**		
SP	0.15	0.19	0.45	0.12	0.40	-0.02	0.25	0.41	0.56	0.50	0.48	0.44	**0.79**	
TM	0.18	0.09	0.41	0.06	0.35	0.07	0.15	0.42	0.51	0.53	0.45	0.47	0.58	**0.71**

4.4. Structure Model Assessment – Structure Equation Modelling

The structure model was tested to estimate the relationships between factors and security culture. The standardized path coefficient (β) and coefficient of determination (R2) were tested. A two-tailed test was computed for t- and p-values at a significance level of 1%, in order to test the significance of the path coefficients. Bootstrapping procedure with a total of 500 cases and 2000 samples was applied to get t-value and determine the path relevance between different hypothetical relationships. A collinearity of structure model was checked first with the help of variance inflation factor (VIF). All VIF values were between 1.02 and 1.95 (see Table 5), which indicated the absence of multicollinearity as the values of VIF are less than 3 (Hair et al. 2016).

The estimated path coefficients β among constructs is displayed below in Figure 2. In a model, all path coefficients are significant at 0.05 except for the paths from extraversion and neuroticism. The strength of the effects exhibits a high level of variation, despite the effect of the majority of correlations being at a significant level. The highly positive significant path was between risk analysis and the security culture (β=0.247, t=4.85); this was followed by top management and security culture (β=0.208,

t=4.84). The lower positive significant path was between openness and security culture (β=0.072, t= 2.12), which was followed by conscientious and security culture (ß=0.075; t =2.240). Table 7 presents the path coefficients β results, *t*-statistics, and significance level p-value for all hypothesised relationships. Also, the results indicated that three dimensions that reflect the security culture have positive significant paths; these are: security awareness, security ownership and security compliance (see below Figure 2). This indicates that the three first-order constructs make a unique contribution to the second one. They provide justification of acceptance of security culture as the second-order factor. The higher path coefficient for security ownership which suggests a greater level of relevance to this dimension, followed by security compliance and security awareness. The determination of coefficient (R2) was estimated to determine the variation percentage in the dependent variable (security culture) explained by independent variables. All different constructs present 69% of security culture's variance.

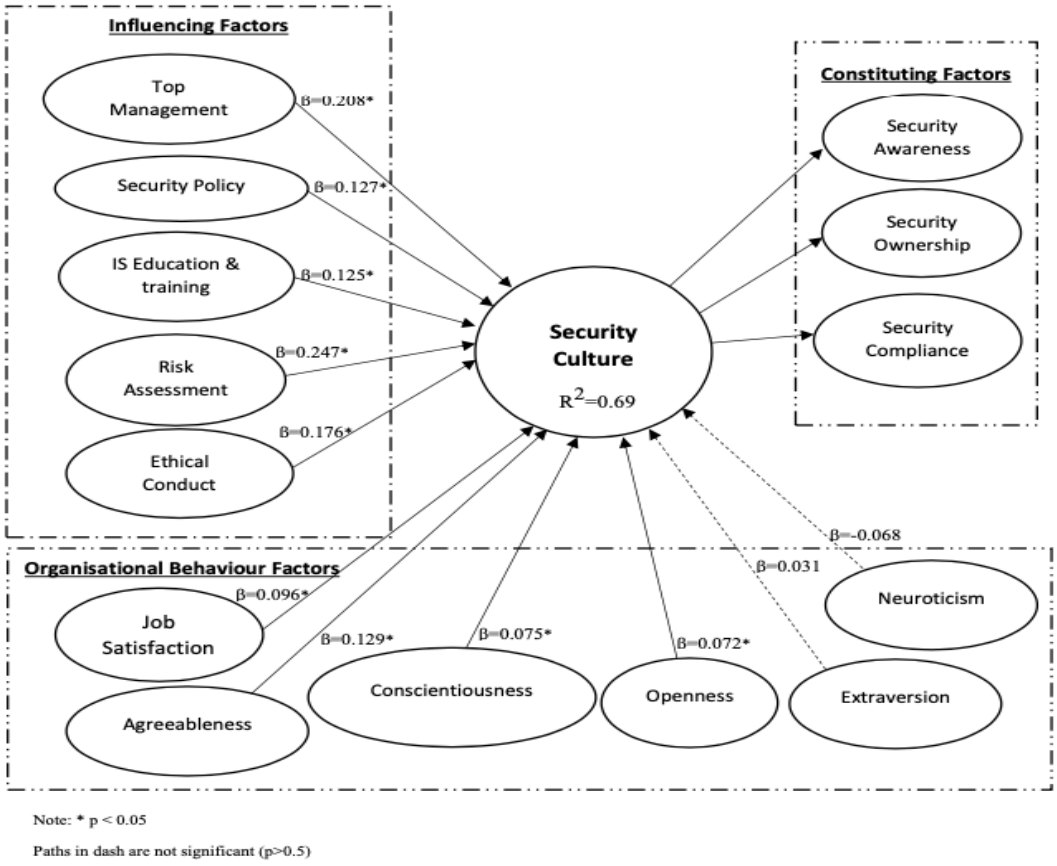

Figure 2. Structure Model

Table 7. Hypotheses Testing

Hypothesis	Path	β	T-value	P-Values	Supported
H1	**TM -> ISC**	0.208	4.843	0.000	Yes
H2	**SP -> ISC**	0.127	2.783	0.006	Yes
H3	**SET -> ISC**	0.125	2.714	0.007	Yes
H4	**RA -> ISC**	0.247	4.856	0.000	Yes
H5	**EC -> ISC**	0.176	3.308	0.001	Yes
H6	**JS -> ISC**	0.096	2.381	0.018	Yes

H7a	**PT-Agr -> ISC**	0.129	3.356	0.001	Yes
H7b	**PT-Con -> ISC**	0.075	2.240	0.025	Yes
H7c	**PT-Ope -> ISC**	0.072	2.126	0.034	Yes
H7d	**PT-Ext -> ISC**	0.031	0.844	0.399	No
H7e	**PT-Neu -> ISC**	-0.068	1.658	0.098	No

Notes: β: Path coefficient, t: t-value, p: p-value; * p < 0.05

4.5. Multi Group Analysis

The subsequent stage was an analysis of the structure model from various forms by focusing on the demographic variables to determine whether the path coefficients' contrasts between groups are relevant statistically. Four demographic variables, that have a sufficient size, were evaluated as moderators between the framework's path relations: organisation type, gender, country, and background education in IT. The sample was split into smaller groups (subsample) and ran separate models for each group. The PLS-MGA method was used to examine the moderators' impacts. The findings indicated that the moderators were significantly supported. However, the demographic variable of background education in IT' fails to have an effect on security culture predictions. The PLS-MGA results show that three differences can be identified for the relationships that exist in regard to security culture between job satisfaction, risk analysis, ethical conduct, security policy and security education. There was a positive significance between job satisfaction and security culture (β=0.20, t=3.18) in the public organisation group; with a nonsignificant (β=- 0.01, t=0.25) in the private organisation group (see below Table 8). Thus, job satisfaction is a vital determinant of security culture effectiveness for public organisation employees, although remains less relevant in private organisations. When comparing gender difference, the path from risk analysis to security culture for male respondents shows a significant positivity (β=0.37, t=4.96); while insignificant positivity and moderate effects for the female group (β=0.11, t=1.98) (see below

Table ***9***). The findings indicated that male employees had higher levels of concern in regard to risk analysis in security culture evaluation compared to female employees.

Table 8.Differences of Organisation Type in PLS-MGA and Path Coefficients

	Private vs Public		**Private**			**Public**		
Path	**diff**	**p-Value**	**β**	**t-Value**	**p-Value**	**β**	**t-Value**	**p-Value**
Agr -> ISC	0.05	0.53	0.13	2.55	0.01	0.08	1.45	0.14
Con -> ISC	0.04	0.56	0.09	1.74	0.08	0.05	1.18	0.23
EC -> ISC	-0.05	0.60	0.11	1.63	0.10	0.16	2.48	0.01
Ext -> ISC	0.14	0.28	0.06	1.40	0.16	-0.08	0.72	0.46
JS -> ISC	**-0.21**	**0.01**	**-0.01**	**0.25**	**0.80**	**0.20**	**3.18**	**0.02**
Neu -> ISC	-0.11	0.25	-0.11	1.35	0.17	0.04	0.08	0.93

Ope -> ISC	0.02	0.69	0.10	2.27	0.02	0.07	1.35	0.17
RA -> ISC	0.07	0.46	0.29	4.21	0	0.21	2.64	0.09
SET -> ISC	0.05	0.55	0.17	2.61	0.09	0.11	1.56	0.11
SP -> ISC	-0.07	0.40	0.08	1.38	0.16	0.15	2.16	0.03
TM -> ISC	0.12	0.17	0.27	4.70	0	0.15	2.09	0.03

Notes: β: Path coefficient, t: t-value, p: p-value; * p < 0.5

Table 9. Differences of Gender in PLS-MGA and Path Coefficients

	Female vs Male		**Female**			**Male**		
Path	**diff**	**p-Value**	**β**	**t-Value**	**p-Value**	**β**	**t-Value**	**p-Value**
Agr -> ISC	0.09	0.21	0.18	3.53	0	0.09	1.53	0.12
Con -> ISC	0.035	0.62	0.08	1.79	0.07	0.05	0.93	0.35
EC -> ISC	-0.07	0.45	0.16	2.28	0.02	0.23	3.56	0
Ext -> ISC	0.07	0.34	0.05	1.08	0.27	-0.02	0.33	0.73
JS -> ISC	-0.02	0.75	0.08	1.72	0.08	0.10	1.72	0.08
Neu -> ISC	0.22	0.08	0.11	1.46	0.14	-0.11	2.12	0.03
Ope -> ISC	0.02	0.78	0.07	1.30	0.19	0.05	1.04	0.29
RA -> ISC	**-0.26**	**0.04**	**0.11**	**1.88**	**0.06**	**0.37**	**4.96**	**0**
SET -> ISC	0.17	0.08	0.20	3.33	0.01	0.03	0.48	0.63
SP -> ISC	0.09	0.30	0.15	2.49	0.01	0.06	0.89	0.37
TM -> ISC	-0.02	0.80	0.19	3.23	0.01	0.22	3.50	0

Notes: β: Path coefficient, t: t-value, p: p-value; * p < 0.5

Also, the study analysed the moderating effect between two countries: United Kingdom and Saudi Arabia. Three differences were revealed through these comparisons (see Table 10). Firstly, the path between ethical conduct and security culture in the United Kingdom group was moderately significant (β=0.16, t=2.10), whereas in Saudi Arabia it was not significant (β=0.14, t=1.79). Second, the path between security education and security culture in the United Kingdom group was shown to be moderately significant (β=0.18, t=2.25), whereas in Saudi Arabia group it was non- significant (β=0.15, t=1.76). Third path was found between security policy and security culture. The path presents a positive significance (β=0.20, t=2.68) in the United Kingdom group; while non-significant positive in Saudi Arabia group (β=0.04, t=0.51). It can be noted that these factors are able to predict organisational security culture and relevance in the United Kingdom.

Table 10. Differences of Country in PLS-MGA and Path Coefficients

	SA vs UK		**SA**			**UK**		
Path	**diff**	**p-Value**	**β**	**t-Value**	**p-Value**	**β**	**t-Value**	**p-Value**
Agr -> ISC	-0.05	0.58	0.12	1.82	0.06	0.18	2.67	0.08
Con -> ISC	-0.01	0.88	0.03	0.45	0.65	0.05	0.69	0.48
EC -> ISC	**-0.21**	**0.04**	**0.14**	**1.79**	**0.07**	**0.16**	**2.10**	**0.03**
Ext -> ISC	0.01	0.94	0.08	1.28	0.19	0.07	0.88	0.37
JS -> ISC	-0.05	0.60	0.04	0.55	0.57	0.09	1.55	0.12

Neu -> ISC	-0.01	0.89	-0.09	1.26	0.20	-0.08	1.00	0.31
Ope -> ISC	0.02	0.79	0.07	1.16	0.24	0.05	0.85	0.39
RA -> ISC	0.06	0.60	0.32	3.88	0	0.26	3.09	0.02
SET -> ISC	**-0.28**	**0.01**	**0.15**	**1.76**	**0.07**	**0.18**	**2.25**	**0.02**
SP -> ISC	**-0.15**	**0.04**	**0.04**	**0.51**	**0.60**	**0.20**	**2.68**	**0.07**
TM -> ISC	0.12	0.24	0.25	3.17	0.02	0.13	1.96	0.05

Notes: β: Path coefficient, t: t-value, p: p-value; * $p < 0.5$

5. Discussion

The aim of the empirical study was to provide validity and reliability to ISCFF using SEM and test hypotheses to identify potential correlations between factors that proved to be important in developing security culture. It showed that the proposed framework is valid, reliable, and achieved an acceptable fit with the data. The quantitative phase provided a rich data sample of 266 employees. The findings confirmed the importance of the identified factors and continue to be significant. The results suggested that influential, organisational behavioural and reflection factors all contribute to a beneficial level of security culture. It also supported the validity of a security culture construct that consists of three dimensions: security awareness, security ownership and security compliance. The influential factors upon security culture in ISCFF were determined as positively predicting these three factors that reflected a security culture. The study added a contribution to other studies in the provision of clarifying the distinction between factors that *reflect* security culture and those factors *influence* it. Also, it can be determined that the findings provide evidence to support prior studies with regard to the beneficial impact of increased job satisfaction levels upon the effectiveness of security culture. The study also added new evidence to existing literature of the significant relationship between personality traits and security culture.

Nine hypothetical relationships presented in

Table ***7*** found support from the empirical results. The samples showed a strong statistical support for how security culture is directly and moderately affected by these factors. As hypothesised, top management support has a positive influence on effectiveness of security culture (H1). Respondents indicated how senior management were dedicated to the improvement of security culture, as well as implementing relevant security training programmes. This finding coincided with previous studies (Greene and D'Arcy 2010; Masrek et al. 2018). It can be concluded that the levels of commitment from top management, combined with strong leadership, function in supporting the advancement of security culture, helps to improve long-term success levels (Nasir et al. 2018). A positive relationship was also found between security policy and security culture (H2). The findings indicated that security policies function in the advancement of quality security culture, and in the implementation of security compliance policy. This finding is in line with studies (Alnatheer 2012; Alhogail 2016). It concluded

that a security culture requires the integration of the development of culture with daily work routines, which will help to increase comprehension levels of employees and how they interact with information security. This will also improve organisations' adaptability levels, and thus, create consistent security policy enforcement techniques. It was evident from the results that there was a lack of access to security policies. 38.7% of respondents did not know how to obtain a copy of their security policies or details of any updated material. This was consistent with the details provided in the interview phase. It is possible to deduce that when an employee has a low level of policy awareness, this can result in noncompliant behaviour.

The testing results from H3 correlated with how security education and training emphasise positivity on security culture. The findings indicated that it is necessary to conduct periodic security training sessions to support employees to achieve specific roles within the development of security culture. As this will reduce the potential risks to information assets, and increase awareness levels, and improve security compliance. This finding is consistent with other studies (Alhogail 2016; Nasir et al. 2018). The findings indicated that security awareness, security education and leadership must be integrated together to ensure the effectiveness of security culture (Martins and Da Veiga 2015). The survey revealed a gap on the efficiency provision of security education and training in organisations. 49.6% of respondents do not know how to find relevant security training programmes in their organisations. 48.5% of respondents had not received any security training sessions during their time at their respective organisations. This correlates with the findings from the interview, as the respondents remarked upon how periodic security training sessions are important to improve security culture. Regarding H4, the security risk analysis and assessment presented a positive effect on security culture. The findings revealed that security risk analysis helps organisations to develop loss, damage awareness, and increase security knowledge to reduce employees' misbehaviour levels, and subsequently improve the level of security culture. The security risk analysis also helps in the provision of employee comprehension levels and how they perceive security in their places of work. This finding is in line with (Alnatheer 2012; Nasir et al. 2018).

A positive effect of ethical codes on security culture was found (H5). The result indicated that ethical conduct functions to guide employees, as they are able to clarify ethical actions. This result supported previous studies to conclude that organisations require to develop ethical codes and notify members about it. Codes of ethical conduct were shown to be an important for security culture development because this helps to support and improve employee behaviour and organisations' acceptance criteria (Alnatheer 2012).The findings confirmed H6 with marked significant correlations between job satisfaction and security culture. The results showed that individuals who report positivity and satisfaction in their jobs commonly comply with security requirements. A higher job satisfaction levels help to develop an increased tendency for security behaviour conformity. The result supported previous studies (Greene and D'Arcy 2010; Farokhi et al. 2016). It can be determined that higher job satisfaction levels help to motivate employees in their compliance with security policies, whilst

simultaneously advancing employees' security awareness and security ownership, to implement security relevance and continuation.

This study examined how the five personality traits effect the development of security culture. The results indicated that three personality traits (agreeableness, conscientiousness, openness) have a significant influential on security culture levels (H7a-H7c). The findings are in line with studies (Pattinson et al. 2015; McBride et al. 2012). The results showed that employees who present with high levels of agreeableness commonly exercise more concerned with security issues, have more acute levels of awareness, which results in more compliant behaviour, and develops a security culture. The findings indicated that conscientiousness in employees develops a higher level of security awareness, with resulting in exercising greater levels of care and maintaining their organisational security cultures. The result revealed that individuals with openness are generally more adept at overcoming challenges through critical thinking. The results indicated that increased levels of openness increase security awareness and compliance that establish an effective security culture. Also, the finding showed that extraversion and neuroticism were not found to be significant influential on security culture; thus, not providing support to H7d and H7e. The findings consistent with (Pattinson et al. 2015; McCormac et al. 2017). It had shown that extraversion and neuroticism did not significantly correlate with self-reported behaviour and security awareness.

The results also provided some evidence that key factors of ISCFF are moderated by organisation type, gender, and country. The demographic characteristics' moderation has been shown to affect job satisfaction levels. It a clearer evidential that job satisfaction levels are a more comprehensive way of predicting a security culture levels of public organisations, although it remains less relevant in private organisations. The study findings demonstrated that male employees, when compared to females, specifically expressed increased levels of concern regarding their organisations' risk analysis and assessment in evaluating security culture. This study also provided analysis of the moderating effects between two nations of United Kingdom and Saudi Arabia. In relation to employees working in the United Kingdom, there was evidential positivity in the correlation between security policies, ethical conduct, security education development and the provision of security culture. It is evident that these particular concepts help in the prediction of security culture and relevance in the United Kingdom.

The SEM results presented the potential ways that researchers and practitioners can direct information security when intending to improve an organisation's level of information security through the use of ISCFF. A framework has presented a comprehensive base for organisations to improve security cultures, which will help in the protection of information assets. It has also been determined that ISCFF components are able to develop a safe work setting that can provide guidance and support in the advancement of security culture. Organisations will be able to improve their employees' behaviour through the implementation of ISCFF. Subsequently, it will be possible to augment security benefits and work against potential threats that employees can pose. This can reduce employees' threats to information security, as guidance will improve their behaviour and change their own values and

perceptions, as based on ISCFF. Also, this will help in the development of security education programmes to raise security awareness levels and improve the security knowledge of employees.

6. Conclusion and Future Work

This research developed an information security culture and key factors framework that combines the most important factors that would increase the understanding of organisational security culture enhancement. The goal of this study was to assess and validate the resulting ISCFF approach. This was achieved through conducting an exploratory survey with 266 valid responses. SEM techniques were implemented to provide results validity to the assessment and test hypotheses. This study has shown that the framework has validity and achieved an acceptable fit with the data to initiate and maintain security culture. The findings confirmed the importance of factors in the framework as vital and effectual upon employees' security culture behaviour. The study provided a base comprehension of factor correlation in regard to the influences upon security culture and factors that reflect it. The findings also support existing literature on positive influence of job satisfaction on the efficiency level of security culture. This study also filled an important gap and added new evidence to existing literature of the significant relationship between personality traits and security culture. The study fulfilled the requirement for additional empirical studies that have focused on security culture cultivation.

The study contributes to improve the knowledge of information security management through the introduction of a comprehensive ISCFF in practice. The framework will help organisations in the development of quality security culture that would help to protect against internal threats. The framework can be used as the base to develop an instrument to measure security culture, as it functions as a comprehensive framework to define relevant items in security culture. Also, the framework practicality is supported in to be the best guideline, which is based on the framework that can be used by security specialists as a reference point in the development of a better security culture. Due to the scope and breadth of the current topic on security culture, there are several limitations for various areas of future research. Future research with larger sample sizes is important to increase the statistical relevance and improve the scope of findings from this study, as well as to confirm that current findings still hold with larger sample. This will assist in gathering rich contextual data in relation of developing information security culture and help to develop the research framework generalisability. It could be beneficial to conduct replica study in a different environment in order to conduct framework testing; this can include different demographics or nationalities.

Also, it would be beneficial to conduct a longitudinal study to collect data from different points of time, as this would provide a better understanding of security culture. Most of the survey items were derived from the literature review, qualitative interviews, and expert reports, as there was a lack of prior survey instruments that can be used for the current study. Consequently, the process for item selection

was not fully objective, although the literature review, interviews and expert reports did reduce the subjectivity levels. There was also a pilot of survey instrument to improve the validity of construct, as the original lack of prior instruments resulted in challenges to the construct operations. Nonetheless, f research is imperative in the process of improving the survey items to develop an automated security culture assessment tool, which would improve the statistical analysis model and data mining models.

Acknowledgements

This work was funded by Saudi Electronic University; the authors are grateful to the funders.

References

Alhogail, A. 2016. "A Framework for the Analysis and Implementation of an Effective Information Security Culture Based on Key Human Factor Elements and Change Management Principles."

Alnatheer, M. 2012. "Understanding and Measuring Information Security Culture in Developing Countries : Case of Saudi Arabia."

Alnatheer, M, T Chan, and K Nelson. 2012. "Understanding And Measuring Information Security Culture." *Pacific Asia Conference on Information Systems (PACIS) 2012*, 144.

Bansal, G. 2011. "Security Concerns in the Nomological Network of Trust and Big 5: First Order vs. Second Order."

Barrick, M.R, M.K Mount, and T.A Judge. 2001. "Personality and Performance at the Beginning of the New Millennium: What Do We Know and Where Do We Go Next?" *International Journal of Selection and Assessment* 9 (1-2): 9–30.

Bartlett, M.S. 1954. "A Note on the Multiplying Factors for Various X2 Approximations." *Journal of the Royal Statistical Society: Series B (Methodological)* 16 (2): 296–98.

Barton, K. A., G Tejay, M Lane, and S Terrell. 2016. "Information System Security Commitment: A Study of External Influences on Senior Management." *Computers and Security* 59: 9–25. https://doi.org/10.1016/j.cose.2016.02.007.

Connolly, L, M Lang, J Gathegi, and D.J Tygar. 2017. "Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour." *Information and Computer Security* 25 (2): 118–36. https://doi.org/10.1108/ICS-03-2017-0013.

DaVeiga, A., and J.H.P Eloff. 2010. "A Framework and Assessment Instrument for Information Security Culture." *Computers & Security* 29 (2): 196–207. https://doi.org/10.1016/j.cose.2009.09.002.

DaVeiga, A. 2018. "An Approach to Information Security Culture Change Combining ADKAR and

the ISCA Questionnaire to Aid Transition to the Desired Culture." *Information and Computer Security* 26 (5): 584–612. https://doi.org/10.1108/ICS-08-2017-0056.

Farokhi, A, S Bahrami, F Esfandnia, M Parvaresh, and S Moradi. 2016. "Review the Relationship between Organizational Culture and Job Satisfaction among Staff of Kermanshah Medical Sciences University in 2014" 10 (1): 88–91.

Goldberg, L.R. 1993. "The Structure of Phenotypic Personality Traits." *American Psychologist* 48 (1): 26.

Greene, G, and J D'Arcy. 2010. "Assessing the Impact of Security Culture and the Emplyee-Organization Relationship in IS Security Compliance." *5th Annual Symposium on Information Assurance (ASIA ' 10),* 42–49.

Hair, J.F, G.T.M Hult, C Ringle, and M Sarstedt. 2016. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage publications.

John, O.P, and S Srivastava. 1999. *The Big-Five Trait Taxonomy: History, Measurement, and Theoretical Perspectives*. Vol. 2. University of California Berkeley.

Kaiser, H. 1974. "An Index of Factorial Simplicity." *Psychometrika* 39 (1): 31–36.

Knapp, K.J., T.E. Marshall, R. K Rainer, and F.N Ford. 2006. "Information Security: Management's Effect on Culture and Policy." *Information Management & Computer Security* 14 (1): 24–36. https://doi.org/10.1108/09685220610648355.

Lowry, P.B, and J Gaskin. 2014. "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It." *IEEE Transactions on Professional Communication* 57 (2): 123–46.

Mahfuth, A. 2019. "Human Factor as Insider Threat in Organizations" 17 (12): 42–47.

Martins, N., and A. Da Veiga. 2015. "An Information Security Culture Model Validated with Structural Equation Modelling." *Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015,* no. Haisa: 11–21.

Masrek, M.N, Q.N Harun, and M.K Zaini. 2018. "The Development of an Information Security Culture Scale for the Development of an Information Security Culture Scale for The." *International Journal of Mechanical Engineering and Technology* 9 (July): 1255–67. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85052730821&partnerID=40&md5=ff35baa9a6ad43a2936fd2fa6fecee69.

McBride, M, L Carter, and M Warkentin. 2012. "Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies." *RTI International-Institute for Homeland Security Solutions* 5 (1): 1.

McCormac, A, T Zwaans, K Parsons, D Calic, M Butavicius, and M Pattinson. 2017. "Individual Differences and Information Security Awareness." *Computers in Human Behavior* 69. https://doi.org/http://dx.doi.org/10.1016/j.chb.2016.11.065.

McCrae, R.R, and O.P John. 1992. "An Introduction to the Five-factor Model and Its Applications."

Journal of Personality 60 (2): 175–215.

Mount, M.K, M.R Barrick, S.M Scullen, and J Rounds. 2005. "Higher-order Dimensions of the Big Five Personality Traits and the Big Six Vocational Interest Types." *Personnel Psychology* 58 (2): 447–78.

Nasir, A, R Arshah, M Hamid, and S Fahmy. 2019. "An Analysis on the Dimensions of Information Security Culture Concept: A Review." *Journal of Information Security and Applications* 44: 12–22. https://doi.org/10.1016/j.jisa.2018.11.003.

Nasir, A, M Rashid, and A Hamid. 2018. "Conceptualizing and Validating Information Security Culture as a Multidimensional Second-Order Formative Construct." *The Thirteenth International Multi-Conference on Computing in the Global Information Technology*, no. c: 1–8.

National Cyber Secuirty Center. 2017. "Growing Positive Security Cultures." 2017. https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures.

Pattinson, M, M Butavicius, K Parsons, A McCormac, and D Calic. 2015. "Factors That Influence Information Security Behavior: An Australian Web-Based Study." In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 231–41. Springer.

PwC. 2013. "The Global State of Information Security." http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml.

Recker, J, M Indulska, M Rosemann, and P Green. 2008. "An Exploratory Study of Process Modelling Practice with Bpmn." *BPM Center Report*.

Roer, K, and G Pertic. 2017. "In Depth Insight into the Human Factor: The Security Culture Report 2017."

Sas, M, W Hardyns, K van Nunen, G Reniers, and K Ponnet. 2020. "Measuring the Security Culture in Organizations: A Systematic Overview of Existing Tools." *Security Journal*. https://doi.org/10.1057/s41284-020-00228-4.

Sas, M, G.L.L. Reniers, W Hardyns, and K Ponnet. 2019. "The Impact of Training Sessions on Security Awareness: Measuring the Security Knowledge, Attitude and Behaviour of Employees." *Chemical Engineering Transactions* 77 (August): 895–900. https://doi.org/10.3303/CET1977150.

Saunders, M, P Lewis, and A Thornhill. 2009. *Research Methods for Business Students*. Pearson education.

Schlienger, T., and S. Teufel. 2003. "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture." *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA* 2003-Janua: 405–9. https://doi.org/10.1109/DEXA.2003.1232055.

Shropshire, J, M Warkentin, A Johnston, and M Schmidt. 2006. "Personality and IT Security: An Application of the Five-Factor Model." *AMCIS 2006 Proceedings*, 415.

Shropshire, J, M Warkentin, and S Sharma. 2015. "Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior." *Computers & Security* 49: 177–91.

Spector, P.E. 1997. *Job Satisfaction: Application, Assessment, Causes, and Consequences*. Vol. 3. Sage.

Tolah, A, S.M. Furnell, and M Papadaki. 2017. "A Comprehensive Framework for Cultivating and Assessing Information Security Culture." *The Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, no. HAISA 2017: 52–64.

Tolah, A, S.M Furnell, and M Papadaki. 2019. "A Comprehensive Framework for Understanding Security Culture in Organizations." *IFIP Advances in Information and Communication Technology* 557: 143–56. https://doi.org/10.1007/978-3-030-23451-5_11.

Vinzi, V.E, L Trinchera, S Amato, J.F Hair Jr, G.T.M Hult, C Ringle, M Sarstedt, P.B Lowry, and J Gaskin. 2016. "PLS Path Modeling: From Foundations to Recent Developments and Open Issues for Model Assessment and Improvement." In *IEEE Transactions on Professional Communication*, 57:123–46. Springer.

Walton, H. 2015. *Security Culture: A How-to Guide for Improving Security Culture and Dealing with People Risk in Your Organisation*. Ashgate Publishing, Ltd.

Wiley, A, A McCormac, and D Calic. 2020. "More than the Individual: Examining the Relationship between Culture and Information Security Awareness." *Computers & Security* 88: 101640.

Appendix A. Research Model Statements

Construct	Survey Items	References
Top Management	TM1: Top management perceives information security as an important organisational priority.	(Knapp et al. 2006)
	TM2: In my organisation, all levels of leadership are always involved in key information security activities.	(Alnatheer 2012)
	TM3: Top managers give strong and consistent support to the security program.	(Knapp et al. 2006)
	TM4: Top managers provide the required resources for training and learning to enable me to comply with information security requirements.	(Alhogail 2016)
	TM5: The involvement and support from top management has a significant role in establishing the security culture.	
Security Policy	SP1: The information security policy clearly states what is expected of me with regard to the safeguarding of information.	(DaVeiga and Eloff 2010)
	SP2: The contents of the information security policy prescribed by my organisation are easy to understand.	(DaVeiga 2018)
	SP3: The information security policy is applicable to the information I use in my daily tasks.	
	SP4: The written information security policy is important to create effective security culture.	Qualitative Data and expert's feedback.
Security Education and Training	SET1: The security-related training program explains what is expected of me, as well as the related information security requirements, policies and how to behave securely from the start of employment.	(Alhogail 2016)
	SET2: I received adequate information security training appropriate for my daily job duties.	(Knapp et al. 2006)
	SET3: I believe that it is necessary to have security refresher training on security policies or any updates in my organisation.	
	SET4: The appropriate information security education and training contribute to creating effective security culture.	(Alhogail 2016)
Risk Analysis and Assessment	RA1: I believe the risk assessment processes of the organisation are adequate to identify risks that negatively impact on information security.	(DaVeiga and Eloff 2010)
	RA2: It is important to understand the security threats, vulnerabilities, and be alerted of any risks inherent to information assets in my workplace.	
	RA3: The security risk analysis and assessment are important in creating an effective security culture.	Qualitative Data and expert's feedback.
Ethical Conduct	EC1: It is important to have a clear ethical code of conduct and direction in protecting sensitive and confidential information by applying related regulations.	(Alhogail 2016)
	EC2: It is important to take care when talking about work or confidential information in public places.	(DaVeiga and Eloff 2010)
	EC3: The security-related ethical code of conduct is important for creating an effective security culture.	Qualitative Data and expert's feedback.
Job Satisfaction	JS1: I feel satisfied with the kind of work I do in this job.	(Spector 1997)
	JS2: I feel I am being paid a fair amount of money for the work I do.	
	JS3: I am satisfied with chances for promotion and rewards.	
	JS4: I am satisfied with the benefits I receive.	
	JS5: I feel satisfied with the organisation's level of supervision.	
	JS6: I like my co-workers.	
Security Awareness	SA1: I am aware of the information security policies and security aspects relating to my job for example, password policy.	(Alhogail 2016)
	SA2: I am aware of ongoing initiatives about security awareness.	
	SA3: It is important to raise awareness about information security with employees.	
Security Ownership	SO1: Protecting information security is the responsibility of every employee in the organisation.	
	SO2: It is important that individuals are involved in the development of security policies in the organisation.	Qualitative Data and expert's feedback.
	SO3: It is important to have a sense of ownership regarding the organisational security practices to enhance the security culture of the organisation.	Qualitative Data and expert's feedback.

Security Compliance	SC1: It is important to follow the information security policies and practices such as not sharing passwords to enhance the security culture in the organisation.	(Alhogail 2016)
	SC2: The organisation enforces adherence to the information security policy.	(DaVeiga and Eloff 2010)
	SC3: I believe that the attention should be drawn on incidents of not adhering to the information security policies and requirements.	

Appendix B. Rotated Factor Loading (Pattern Matrix)

	Component													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
SP1	0.80													
SP2	0.85													
SP3	0.80													
SP4	0.69													
TM1		0.76												
TM2		0.75												
TM4		0.67												
TM5		0.66												
SO1			0.82											
SO2			0.81											
SO3			0.84											
SA1				0.80										
SA2				0.71										
SA3				0.80										
SC1					0.82									
SC2					0.74									
SC3					0.70									
SET1						0.66								
SET3						0.74								
SET4						0.79								
RA1							0.51							
RA2							0.88							
RA3							0.86							
JS1								0.78						
JS2								0.71						
JS4								0.71						
JS5								0.78						
JS6								0.71						
Neu1									0.51					
Neu2									0.88					
Neu3									0.85					
Neu4									0.82					
Neu5									0.86					
Neu6									0.50					
Neu7									0.85					
Neu8									0.51					
Ope1										0.84				
Ope2										0.59				

Ope3										0.51				
Ope4										0.73				
Ope5										0.73				
Ope6										0.71				
Ope7										0.62				
Ope8										0.76				
Ope9										0.51				
Ope10										0.51				
Agr1											0.81			
Agr2											0.81			
Agr3											0.70			
Agr4											0.55			
Agr5											0.66			
Agr6											0.50			
Agr7											0.50			
Agr8											0.76			
Agr9											0.75			
Con1												0.72		
Con2												0.73		
Con3												0.69		
Con4												0.68		
Con5												0.64		
Con6												0.77		
Con7												0.73		
Con8												0.50		
Con9												0.51		
EC1													0.86	
EC2													0.90	
EC3													0.90	
Ext1														0.72
Ext2														0.77
Ext3														0.75
Ext4														0.80
Ext5														0.80
Ext6														0.50
Ext7														0.51
Ext8														0.75
Eigen Value	11.6	5.3	4.2	3.9	3.5	3.2	2.7	2.1	1.9	1.7	1.7	1.5	1.4	1.4
Variance (%)	14.9	6.8	5.4	5.0	4.5	4.1	3.5	2.7	2.4	2.2	2.1	2.0	1.8	1.7
Cumulative Variance explained	14.9	21.7	27.2	32.2	36.6	40.7	44.2	47	49.4	51.6	53.8	55.8	57.6	59.4

Appendix C. Factor Loading with Cross Loading

	Agr	Con	EC	Ext	JS	Neu	Ope	RA	SA	SC	SET	SO	SP	TM
Agr1	**0.81**	0.22	0.21	0.01	0.11	0.05	0.24	0.21	0.24	0.32	0.21	0.33	0.16	0.22
Agr2	**0.81**	0.17	0.23	0.00	0.08	-0.01	0.26	0.15	0.23	0.22	0.16	0.24	0.07	0.13
Agr3	**0.70**	0.19	0.17	0.07	0.08	-0.04	0.21	0.13	0.16	0.18	0.08	0.24	0.04	0.08
Agr4	**0.55**	0.05	0.16	0.06	0.16	-0.04	0.15	0.10	0.18	0.14	0.11	0.14	0.14	0.07
Agr5	**0.66**	0.16	0.18	-0.04	0.06	0.03	0.05	0.24	0.19	0.18	0.14	0.21	0.17	0.09
Agr8	**0.76**	0.15	0.21	-0.06	0.10	0.04	0.16	0.17	0.19	0.25	0.18	0.27	0.13	0.19
Agr9	**0.75**	0.16	0.23	-0.01	0.02	0.00	0.23	0.13	0.26	0.19	0.16	0.23	0.06	0.11
Con1	0.26	**0.72**	0.27	0.09	0.18	-0.03	0.40	0.24	0.21	0.32	0.28	0.33	0.21	0.12
Con2	0.16	**0.73**	0.18	0.09	0.10	-0.02	0.20	0.17	0.11	0.19	0.14	0.20	0.11	0.00
Con3	0.07	**0.69**	0.11	0.07	0.06	-0.10	0.15	0.08	0.09	0.14	0.16	0.16	0.11	0.00
Con4	0.04	**0.68**	0.05	-0.02	0.05	-0.13	0.09	0.09	0.09	0.15	0.13	0.21	0.11	0.08
Con5	0.06	**0.64**	0.01	0.02	-0.03	-0.14	-0.01	0.01	0.00	0.07	0.11	0.16	0.08	0.03
Con6	0.16	**0.77**	0.07	0.07	0.01	-0.15	0.08	0.10	0.13	0.19	0.19	0.18	0.14	0.09
Con7	0.22	**0.73**	0.12	0.05	0.01	-0.04	0.17	0.14	0.15	0.18	0.15	0.17	0.11	0.11
EC1	0.20	0.17	**0.86**	0.14	0.19	0.01	0.24	0.46	0.42	0.53	0.40	0.41	0.32	0.38
EC2	0.23	0.12	**0.90**	0.18	0.21	-0.05	0.20	0.49	0.45	0.54	0.45	0.47	0.41	0.34
EC3	0.30	0.23	**0.90**	0.15	0.27	-0.04	0.32	0.53	0.45	0.52	0.50	0.45	0.46	0.38
Ext1	-0.02	0.04	0.11	**0.72**	0.06	0.11	0.07	0.12	0.10	0.14	0.03	0.03	0.10	0.06
Ext2	0.07	0.11	0.10	**0.77**	0.05	-0.04	0.08	0.06	0.07	0.16	0.02	0.02	0.03	0.06
Ext3	-0.01	0.06	0.09	**0.75**	0.02	0.04	0.13	0.06	0.11	0.12	0.05	-0.06	0.12	0.00
Ext4	0.01	0.09	0.20	**0.80**	0.06	0.03	0.09	0.06	0.11	0.19	0.06	0.04	0.10	0.10
Ext5	0.00	0.05	0.15	**0.80**	0.06	0.06	0.09	0.12	0.21	0.15	0.07	0.03	0.15	0.03
Ext8	-0.05	0.04	0.13	**0.75**	0.02	0.04	0.14	0.02	0.03	0.13	0.03	0.00	0.07	0.04
JS1	0.08	0.10	0.20	0.05	**0.78**	-0.02	0.24	0.20	0.32	0.32	0.23	0.28	0.33	0.30
JS2	0.16	0.07	0.19	0.04	**0.71**	-0.07	0.15	0.22	0.29	0.29	0.23	0.27	0.28	0.28
JS4	0.06	0.04	0.18	0.11	**0.71**	0.01	0.11	0.25	0.18	0.27	0.19	0.21	0.21	0.25
JS5	-0.02	0.04	0.20	0.05	**0.78**	0.01	0.21	0.23	0.12	0.33	0.19	0.22	0.34	0.28
JS6	0.12	0.10	0.16	-0.01	**0.71**	-0.08	0.27	0.18	0.23	0.32	0.22	0.26	0.32	0.21
Neu2	0.06	-0.11	-0.02	-0.11	-0.02	**0.88**	0.04	-0.03	-0.03	-0.09	-0.11	-0.09	-0.01	-0.01
Neu3	0.05	-0.09	-0.04	0.01	0.02	**0.85**	0.00	-0.03	-0.07	-0.08	-0.06	-0.06	-0.01	0.01
Neu4	-0.05	-0.11	0.03	0.04	-0.06	**0.82**	0.02	0.05	-0.02	-0.03	-0.06	-0.07	0.05	0.03
Neu5	-0.02	-0.08	-0.07	0.08	-0.06	**0.86**	0.04	-0.08	-0.15	-0.07	-0.12	-0.12	-0.10	-0.01
Neu7	0.03	-0.05	0.08	0.06	-0.03	**0.85**	0.04	-0.04	0.00	-0.02	-0.09	-0.06	-0.01	0.09
Ope1	0.22	0.14	0.21	0.08	0.23	-0.03	**0.84**	0.19	0.18	0.25	0.17	0.25	0.15	0.13
Ope2	0.26	0.46	0.29	0.15	0.22	0.04	**0.59**	0.24	0.25	0.38	0.27	0.30	0.21	0.16
Ope4	0.15	0.16	0.20	0.09	0.15	0.02	**0.73**	0.15	0.20	0.20	0.15	0.19	0.23	0.10
Ope5	0.19	0.05	0.09	0.05	0.18	0.04	**0.73**	0.11	0.10	0.13	0.08	0.15	0.12	0.02
Ope6	0.11	0.09	0.23	0.10	0.19	-0.05	**0.71**	0.17	0.14	0.21	0.19	0.16	0.25	0.14
Ope7	0.13	0.10	0.15	0.04	0.12	0.02	**0.62**	0.07	0.17	0.20	0.13	0.20	0.15	0.10

Ope8	0.17	0.13	0.15	0.05	0.22	-0.04	**0.76**	0.16	0.16	0.20	0.14	0.24	0.15	0.08
Ope10	0.11	0.16	0.30	0.08	0.13	-0.11	**0.51**	0.17	0.12	0.24	0.19	0.16	0.26	0.03
RA1	0.11	0.03	0.22	0.08	0.14	0.07	0.23	**0.51**	0.26	0.28	0.25	0.21	0.31	0.28
RA2	0.17	0.17	0.52	0.10	0.26	-0.06	0.15	**0.88**	0.49	0.54	0.48	0.49	0.39	0.37
RA3	0.22	0.21	0.48	0.07	0.22	-0.10	0.21	**0.86**	0.42	0.52	0.48	0.47	0.28	0.33
SA1	0.24	0.16	0.37	0.12	0.26	-0.01	0.21	0.36	**0.80**	0.45	0.36	0.43	0.52	0.45
SA2	0.12	0.07	0.31	0.12	0.23	0.02	0.14	0.33	**0.71**	0.34	0.36	0.28	0.42	0.39
SA3	0.28	0.17	0.46	0.12	0.25	-0.16	0.23	0.51	**0.80**	0.52	0.53	0.54	0.36	0.36
SC1	0.25	0.25	0.58	0.14	0.33	-0.18	0.27	0.62	0.54	**0.82**	0.48	0.64	0.38	0.40
SC2	0.24	0.22	0.37	0.16	0.30	0.02	0.29	0.38	0.40	**0.74**	0.35	0.41	0.48	0.47
SC3	0.19	0.15	0.36	0.17	0.31	-0.01	0.22	0.31	0.33	**0.70**	0.35	0.32	0.29	0.34
SET1	0.19	0.17	0.28	0.02	0.28	0.00	0.13	0.27	0.41	0.35	**0.66**	0.35	0.47	0.45
SET3	0.10	0.17	0.37	0.09	0.14	-0.11	0.16	0.39	0.40	0.39	**0.74**	0.32	0.27	0.24
SET4	0.17	0.22	0.46	0.02	0.21	-0.11	0.24	0.52	0.40	0.42	**0.79**	0.38	0.32	0.30
SO1	0.27	0.30	0.49	0.10	0.33	-0.10	0.28	0.52	0.51	0.60	0.47	**0.82**	0.41	0.43
SO2	0.27	0.22	0.38	-0.08	0.25	-0.08	0.24	0.38	0.43	0.49	0.34	**0.81**	0.37	0.38
SO3	0.29	0.22	0.35	0.03	0.26	-0.10	0.26	0.41	0.42	0.45	0.37	**0.84**	0.32	0.36
SP1	0.12	0.12	0.39	0.11	0.34	0.00	0.19	0.30	0.49	0.39	0.37	0.37	**0.80**	0.44
SP2	0.07	0.14	0.32	0.04	0.35	-0.04	0.20	0.33	0.43	0.38	0.33	0.34	**0.85**	0.53
SP3	0.08	0.13	0.28	0.16	0.33	-0.04	0.17	0.23	0.42	0.34	0.37	0.31	**0.80**	0.47
SP4	0.19	0.22	0.41	0.10	0.26	0.00	0.25	0.43	0.42	0.46	0.44	0.38	**0.69**	0.42
TM1	0.14	0.11	0.37	0.10	0.27	-0.02	0.13	0.37	0.45	0.47	0.32	0.44	0.49	**0.76**
TM2	0.10	0.04	0.29	0.09	0.27	0.00	0.10	0.25	0.31	0.37	0.25	0.31	0.46	**0.75**
TM4	0.12	0.00	0.21	-0.04	0.23	0.01	0.10	0.21	0.31	0.32	0.31	0.27	0.38	**0.67**
TM5	0.17	0.11	0.28	0.00	0.25	0.05	0.12	0.34	0.36	0.34	0.41	0.31	0.32	**0.66**