7-15-2012

Understanding And Measuring Information Security Culture

Mohammed Alnatheer
Information Security Institute, Queensland University of Technology, Australia, mohammed.alnatheer@student.qut.edu.au

Taizan Chan
Faculty of Science and Engineering, Queensland University of Technology, Australia, t.chan@qut.edu.au

Karen Nelson
Faculty of Science and Engineering, Queensland University of Technology, Australia, kj.nelson@qut.edu.au

UNDERSTANDING AND MEASURING INFORMATION SECURITY CULTURE

Mohammed Alnatheer, Information Security Institute, Queensland University of Technology, Australia, mohammed.alnatheer@student.qut.edu.au

Taizan Chan, Faculty of Science and Engineering, Queensland University of Technology, Australia, t.chan@qut.edu.au

Karen Nelson, Faculty of Science and Engineering, Queensland University of Technology, Australia, kj.nelson@qut.edu.au

Abstract

The purpose of the current paper was to develop a measurement of information security culture. Our literature analysis indicated a lack of clear conceptualization and distinction between factors that constitute information security culture and factors that influence information security culture. A sequential mixed method consisting of a qualitative phase to explore the conceptualisation of information security culture, and a quantitative phase to validate the model is adopted for this research. Eight interviews with information security experts in eight different Saudi organisations were conducted, revealing that security culture can be constituted as reflection of security awareness and security ownership. Additionally, the qualitative interviews have revealed that factors that influence security culture are top management involvement, policy enforcement, and training. These factors were confirmed formed the basis for our initial information security culture model, which was operationalised and tested in different Saudi Arabian organisations. Using data from two hundred and fifty-four valid responses, we demonstrated the validity and reliability of the information security culture model. We were further able to demonstrate the validity of the model in a nomological net, as well as provide some preliminary findings on the factors that influence information security culture.

Keywords: Security Culture, Factors Influence Security Culture, Factors Constitute Security Culture

1 INTRODUCTION

One of the major benefits of information security culture creation is the protection of the organization assets in which will have "direct interaction with information assets and thereby minimize the threats that user behaviour poses to the protection of information assets" (Da Veiga, 2008) (p.1). The importance of creating a security culture within organization settings arises from the fact that the human dimension in information security is always considered to be the weakest link (Da Veiga. & Eloff, 2007; Martins & Eloff, 2002; Maynard & Ruighaver, 2002; Schlienger & Teufel, 2003, van Niekerk. & von Solms, 2005). Therefore, the creation of an information security culture is necessary for effective information security management (J. Eloff & Eloff, 2005; M. Eloff & von Solms, 2000). The current paper has reviewed some common security culture definitions in order to gain understanding of what constitute security culture. Some of the definitions found for security culture are:

- Schlienger and Teufel (2003) (P.405) state that information security culture is "a subculture in regards to content". They declare:
  Security culture encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee.
- Dhillon, (1999)(P.90) defines security culture as:
  The totality of human attributes such as behaviours, attitudes and values that contribute to the protection of all kinds of information in a given organisation.
- Von Solms (2000) (p.618) calls for security culture creation within organization: By instilling the aspects of information security to every employee as a natural way of performing his or her daily job.

Despite the importance of the previous definitions in recognising the need to create security culture in order to manage security effectively, there is little information about what constitutes or conceptualizes security culture (Ramachandran, Srinivasan, & Goles, 2004). The definitions did not offer a clear understanding of what constituted or conceptualized security culture. This general lack of agreement on just what constitutes a security culture presents a dilemma in terms of identifying factors or elements that are necessary for the creation of a security culture. This paper attempts to fill this gap by developing an information security culture measurement model that will conceptualize security culture.

2 MODEL AND HYPOTHESES DEVELOPMENT

A comprehensive review of information security culture was conducted in order to develop an understanding of information security culture measurement. The purpose of the comprehensive review is to identify and examine factors that constitutes or reflect security culture and factors that influence security culture in order to develop information security culture measurement model. The findings of this review indicated there are only two information security culture research models that have provided a reliable and valid information security culture assessment instrument (Da Veiga & Eloff, 2009; Schlienger & Teufel, 2003). In the first of these, Schlienger and Teufel (2005) designed a questionnaire to obtain an understanding of official rules intended to influence the security behaviour of employees. In the second, an instrument was developed by Da Veiga, and Eloff (2009) designed to cultivate information security culture.

The existing literature has emphasized the importance of information security culture and provided suggestions and guidelines on how to assess information security culture. However, the findings of the comprehensive review revealed that there is little clarification as to what exact factors constitute security culture and as to what factors influence or drive the creation of security culture. The distinction clearly has not been made by academic literature on the information security culture. These literature analyses have not provided a clear understanding of how security culture must be conceptualized in order for researchers to develop an instrument for the understanding and

measurement of an information security culture model. Therefore, the comprehensive review illustrated the lack of empirical measurement in the information security culture area. As a result, the current paper will take this initiative and develop an information security culture measurement model that clearly distinguishes between what factors constitute security culture and what factors influence or drive the security culture. In order to achieve this goal, an open ended interview will be implemented to develop the information security culture measurement model.

2.1 Qualitative Data Findings

This paper conducted eight separate interviews from eight different organisations across public, semi-pubic, and private sectors; different sizes were also included, ranging from small to large organisations. Table 1 presented the demographic information profile for each organization. The participants' roles however were as information security managers or as experts in their respective organisations. Because of space and scope limitations, the current paper would not discuss the qualitative interviews findings analysis in details.

Organisation	Organisation Type	Organisation Size	Type of Industry
A	Semi-Public	400	Government Regulators
B	Private	800	Consulting, Auditing, Assurance
C	Private	3100	IT, Network, System
D	Semi-Public	100	IT
E	Semi-Public	1150	Health, Education, Research
F	Public	3000	Healthcare
G	Private	1000	Banking and Financial
H	Private	3000	Banking and Financial

Table 1. Demographic Information Profile

2.1.1 Factors constitute security culture

Based on the qualitative interviews findings, security culture was constituted as reflection of security awareness and security ownership. Some quotes are provided below

On Security Awareness:
In order to change the security culture, we need to improve our security awareness around here (Organization A).
On Security Ownership:
We do not expect to create security culture in my organization since our staffs do not understand the importance of protecting information security (Organization F).

2.1.2 Factors influence security culture

Based on the qualitative interviews findings, factors influence security culture is top management involvement in information security, information security policy enforcement and security training.

On Top Management Involvement:
Excellent top management participations and involvement is the most important factors for creating information security culture (Organization H).

To create or expect some sort of security culture, top management must be involved.

(Organization E).

On Policy Enforcement:
One of the key factors for effective information security culture in my organization is being able to enforce the security policy (Organization D).

On security training:

Security training is the one of effective and successful factors for establishing information security culture in my organization (Organization B).

2.2 Factors Constituting Security Culture

2.2.1 Security awareness

Siponen (2000) (p.31) defined security awareness as "A state where users in an organisation are aware, ideally committed to, of their security mission". Security awareness has been well acknowledged in the literature to be an essential component for creating security culture. Von Solms (2000) refers to the third wave of information security, called the institutionalization wave, often discussed under the title *"information security awareness"* and more recently under the title *"information security culture"*. Earlier researchers referred to security culture as advanced stages of security awareness of organisations. Instilling a security culture is achieved through security awareness, knowledge and skills (Tarimo, 2006). The importance of security awareness for the establishment of a security culture has been acknowledged by other researchers in the literature. For example, van Niekerk and von Solms, (2005) state that as security culture is closely related to security behaviour, analysing security awareness levels will directly contribute to the establishment and maintenance of a security culture. The ISO/IEC standard states that security awareness of all employees is an essential element of effective security and contributes positively to an improved security culture (International Standards Organization ISO/IEC TR 13335-1, 2004).

2.2.2 Security Ownership

It is important for staff in any organisation to understand their security roles and responsibilities, in order to enhance their security performance and thus the organisation's security performance. By understanding their responsibilities and the importance of protecting information security, staffs are able to understand what security risks are associated with their actions. This will increase their security awareness levels, which will increase compliance with the security policy of the organisation. For this reason, employee responsibility and ownership of the need to protect information security is an important aspect of creating a security culture (Koh et al., 2005; Maynard & Ruighaver, 2002; Ramachandran et al., 2004; Tarimo, 2006). By being responsible and having a sense of ownership, staff behaviour will change with respect to protecting organisational assets, leading to the creation of a security culture.

2.3 Factors Influencing Security Culture

2.3.1 Top Management Involvement in Information Security

Fourie (2003) indicated that top management can be involved by defining and communicating a security policy, allocating specific responsibilities to appointed people, making resources available for the continual upkeep of information security and control, and constantly monitoring and reviewing information security effectiveness. Many researchers have asserted that top management is an essential part of the establishment of a security culture (Chia et al., 2003; D'Arcy & Greene, 2009; Da Veiga & Eloff, 2007, 2009; Dojkovski et al., 2007; Kraemer, Carayon, & Clem, 2009; Martins & Eloff, 2002; Maynard & Ruighaver, 2002; OECD, 2003; Schlienger & Teufel, 2003, 2005; Tarimo, 2006; van Niekerk & von Solms, 2005, 2006). Gaunt (2000) argued that when creating an information security culture, commitment from the management and strong leadership is necessary at an initial stage to succeed in the long term. In addition, Knapp, et al (2006) found that top management support is the most important significant predictor of security culture and level of policy enforcement. A security culture would not be easily established without strong and consistent involvement from the top management of the organisation.

2.3.2 Information Security Policy Enforcement

A security policy is important for the creation of a security culture. OECD (2003) reports that for security awareness to succeed, it needs a foundation of security policies. Security policies are extremely important and should be included in an organisation's information security program. It is important to cultivate an information security culture in an organisation and understand how the

culture can be integrated with the security policy (Kluge, 1998). This is important because the superficial goal of security culture is to influence the behaviour of the employees to comply with the official security policy (Schlienger & Teufel, 2003). Nevertheless, even though some organisations have an established security policy, this does not ensure that employees will necessarily obey these policies (Von Solms & von Solms, 2004). Therefore, consistent enforcement of the security policy will assist the effectiveness of information security policy and must be an organisational priority in order to create security mind culture.

2.3.3 Information Security Training

Organisations need to ensure that "an information security culture is inculcated through training, education and awareness raising, in order to minimize risks to information assets" (Da Veiga & Eloff, 2007) (P.149). This implication conforms to the assertion that an effective security culture represents one of the necessary foundations for information security management and cannot be achieved without appropriate attention to security awareness, training and education for all ICT users (Tarimo, 2006). Companies can be assisted to establish a security culture through various approaches that are based on policy, awareness, training and education (Furnell, Gennatou, & Dowland, 2001; Lichtenstein & Swatman, 2001; Lim, Ahmad, Chang, & Maynard, 2010; Schlienger & Teufel, 2003). Education of employees in terms of their security roles and responsibilities is a crucial aspect of security culture (R. von Solms & S. von Solms, 2004). Security training can contribute to the security culture creation by improving employees' behaviour and increasing their security awareness levels. This might be reflected in their security behaviour should they then follow the security policy which initially gave rise to the necessary creation of the security culture.

Based on the previous discussion the following hypotheses were emerged:

- HI: Security culture is constituted mainly of two reflective factors: (a) Security Awareness, (b) Security Ownership.
- H2: Top Management Involvement, Information Security Policy Enforcement, and Information Security Training are factors that have positive and significant influence on security culture.

Figure 1 depicts the developed information security culture measurement model based on the qualitative interviews findings and the synthesized literature review.

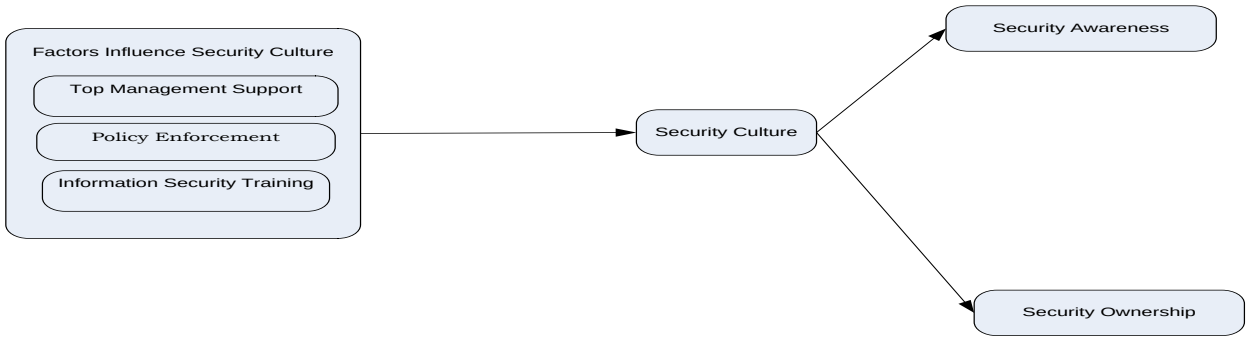

Figure 1. Information Security Culture Model

3 RESEARCH METHODOLOGY

3.1 Construction of Scales

The scales were developed through an iterative process of extracting candidate questionnaire items directly from the interview response questions and the panel experts' feedback. It is advisable to adapt measurement scales of these constructs. This consideration of scale items helps to assure content validity (Nunnally & Bernstein, 1994). Therefore, a significant number of the scales used were adapted from previous reliable and validated instruments (D'Arcy & Greene, 2009; Da Veiga. et al., 2007; Knapp. et al., 2006). However, the qualitative interviews and expert panel judgments have suggested the need to add more item scales for each construct to demonstrate the appropriate constructs. Moreover, the security ownership construct was constructed since there was a lack of academic representation for the security ownership construct. Please note the items derived from the qualitative interviews findings were not discussed in this paper because of the scope limitation.
For each of these constructs, pools of candidate items were generated from the literature (i e, D'Arcy & Greene, 2009; Da Veiga. et al., 2007; Knapp. et al., 2006), qualitative interviews findings, and panel experts feedback to add more scales in order to develop the appropriate theoretical constructs. After creating the items needed to develop the theoretical constructs, the items were worded in the form of a statement to which the respondent indicated his/her perception of the extent of agreement on a 5-point likert scale with the end points 'strongly disagree' and 'strongly agree'.

3.2 Expert Panel and Instrument Refinement

After generation of the initial pools of candidate items was the establishment if the construct validity of the candidate items to display the convergent and discriminant validity. The current paper followed the recommendations of Moore and Benbasat's (1991) study which employed 'Own Category Test' to ensure the construct validity (Davis, 1989; Sherif & Sherif, 1967). This can be achieved by asking a panel of experts with a strong background in information security system records to sort candidate items into a number of constructs to ensure the identify domain substrata of the primary theatrical constructs (Moore & Benbasat, 1991; Recker, 2008). Each panel member was asked to place the candidate items in the correspondent constructs. This helped to assess the convergence and representativeness of the items. It is also important to assess whether panel members placed the same candidate items in the respective constructs. This ensured cluster reliability demonstration by assessing the items placed in the target constructs across all members (Recker, 2008). All of the items were found categorized in the correspondent constructs according to the panel expert's categorizations.
Afterwards, a pool of candidate items was reduced to the potential candidate items in order to improve the validity and reliability of the final set of items. This was achieved by following the index card sorting test which was established by (Davis, 1989; Moore & Benbasat, 1991). If any items were found within a particular category, then it demonstrated convergent validity with the construct associated with the category, and discriminant validity with the others (Recker, 2008). This sorting test was conducted by a panel of four judges with a strong background in information system securities that had randomly given items on printing index cards and were asked to sort these cards into categories. The panel of judges were asked to classify items into given categories and identify items that were ambiguous. This approach ensured highly reliable and valid instruments.
After revising the questionnaires, pilot testing was conducted with twenty participants from Saudi Arabian organisations to evaluate the questionnaire for clarity, bias, ambiguous questions and relevance to the Saudi Arabian business environment. Fifteen respondents offered valid feedback that was considered sufficient for serving the purpose (Burns & Bush, 1998). The operational details of the security factors influence security culture constructs and factors constitutes security culture, in terms of the dimensions along with the measurement variables and references, are presented in Table 2.

Dimension		Measurement Variables	References
Top Management	TPM1	Top management considers information security an important organisational priority	(Knapp et al., 2006)

Involvement In Information Security	TPM2	Senior management gives strong and consistent support to the security program	(Knapp et al., 2006)
	TPM3	Senior management is always involved in key information security activities.	Qualitative Data* and experts feedback/input
	TPM4	Management ensures that appropriate individuals are made responsible for specific aspects of information security	Qualitative Data* and experts feedback/input
	TPM5	Management ensures that everyone who takes information security actions, and makes information security decisions and are held accountable for their decisions and actions	Qualitative Data* and experts feedback/input
Information Security Policy Enforcements	PE1	Information security practices and procedures are continually monitored to ensure compliance with security policy	(Da Veiga, Martin, and Eloff, 2007)
	PE2	Information security practices and procedures are externally audited	Qualitative Data* and experts feedback/input
	PE3	Information security violations are reported to the proper authority	(Knapp et al., 2007)
	PE4	Actions against violations are always taken	Qualitative Data* and experts feedback/input
Information Security Training	T1	I receive adequate information security training	(D'Arcy and Greene, 2009)
	T2	Information security policy is communicated well	Qualitative Data* and experts feedback/input
	T3	I am always educated or trained about new security policies	(Knapp et al., 2007)
Information Security Awareness	AW1	I am aware of my information security roles and responsibilities	(Chalua, 2006)
	AW2	I am aware of the risk of not following the information security policy	Qualitative Data* and experts feedback/input
	AW3	I am familiar with the information security policy	Qualitative Data* and experts feedback/input
	AW4	I am aware of the procedures for reporting security policy violations	(D'Arcy and Greene, 2009)
Information Security Ownerships	OWN1	It is my responsibility to protect the information of my organisation	Qualitative Data* and experts feedback/input
	OWN2	I take ownership of the outcomes of my information security decisions and actions	
	OWN3	Protecting information security is an important part of my job	

*: Items Derived from Qualitative Data are beyond the scope of this paper

Table 2. Research Model Construct Operationalisation Statements

3.3 Questionnaires Administration

A questionnaire survey was conducted in Saudi Arabia from March to May 2010. Postal mail was chosen as the primary means of distributing the survey instrument. To improve the response rate, a web-based version of the questionnaire was also developed as an alternative method for respondents to use. The survey packages (a cover letter explaining the purposes and benefits of the survey, and a set of questions) were mailed to 200 Saudi Arabian organisations covering all the country's regions, types and sizes. Respondents came from a variety of organisational levels, geographic locations, backgrounds, education levels and ages. One hundred and fifty questionnaires were returned by mail and one hundred and fifty surveys were completed online. Forty-six of the returned questionnaires

were excluded from the analysis, due to significant incompletion. As a result, 254 valid responses from 64 organisations remained. A 32 per cent response rate is considered satisfactory for research conducted in the information security field (Kotulic & Clark, 2004). The profiles of the survey sample respondents are summarized in Table 3. Table 4 demonstrated the descriptive statistics for each statement in our research model.

	%		%		%
Organisation Type		Organisation Size		Organisation Industry	
Private	48.8	1-499	24.8	Financial	18.9
Public	29.5	500-4999	40.9	Education	14.2
Non- Profit	1.2	more than 5000	34.3	Telecommunications	10.6
Semi-Public	20.5	Participants Age		IT	9.4
Job Title		21-30	46.9	Insurance	8.7
Security Staff	13.4	31-40	39.8	Health are	8.3
IT Staff	39.8	41-50	11.0	Construction	7.1
Users Staff	46.9	51-60	2.4	Others	22.9

Table 3. Frequencies of Demographic Variables

Variable	Mean	SD	SE	Variable	Mean	SD	SE
TPM1	4.10	.94	.059	T1	2.83	1.13	.081
TPM2	3.88	.98	.062	T2	3.18	.94	.068
TPM3	3.54	1.05	.067	T3	2.83	.98	.076
TPM4	3.58	1.12	.071	AW1	3.72	1.03	.065
TPM5	3.61	1.04	.065	AW2	3.87	1.01	.064
PE1	3.64	1.08	.068	AW3	3.63	1.03	.066
PE2	3.33	1.13	.074	AW4	3.28	1.14	.073
PE3	3.43	.94	.071	OWN1	3.99	1.0	.068
PE4	3.42	.98	.067	OWN2	3.98	.96	.061
				OWN3	4.04	1.0	.067

Table 4. Descriptive Statistic for Model statements

4 MODEL RELIABILITY AND VALIDITY

To ensure that such a set of measurement scales consistently and accurately captured the meaning of the constructs, an analysis of scale reliability was performed through an assessment of internal consistency (Cronbach's alpha coefficient) and inter-total correlations (Pallant, 2005). The values of the alpha Cronbach's coefficient of all the construct scales ranged from 0.847 to 0.906, suggesting good internal consistency and reliability for the scales with this sample (See Table 5). Additionally, the results of item-total correlations presented in Tables 6 show that all of the variables within each construct measure the actual construct, as their corrected item-total correlations were greater than 0.30.

Constructs Measurement Scale	Number of Variables	Cronbach's Alpha	Constructs Measurement Scale	Number of Variables	Cronbach's Alpha
Top Management Involvement	5	.870	Awareness	4	.906
Policy Enforcement	4	.820	Ownership	3	.847
Training	3	.842			

Table 5. Cronbach's alphas of measurement scales for Each Construct

Variables	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Variables	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
TPM1	.740	.833	T1	.701	.787
TPM2	.774	.824	T2	.671	.814

TPM3	.740	.831	T3	.751	.737
TPM4	.637	.859	AW1	.814	.869
TPM5	.602	.865	AW2	.806	.873
PE1	.563	.783	AW3	.820	.867
PE2	.685	.810	AW4	.722	.905
PE3	.704	.754	OWN1	.737	.766
PE4		.746	OWN2	.686	.826
			OWN3	.726	.776

Table 6. Item-total correlations of all statements

Afterwards, validity was achieved using EFA and CFA. EFA is particularly useful as a preliminary analysis in the absence of a sufficiently detailed theory about the relations of the variables to the underlying constructs (Gerbing & Anderson, 1988). The factorability refers to the suitability of the data to be factorized in terms of the inter-correlation between variables (Pallant, 2005; Tabachnick & Fidell, 2007). As the variables included in the analysis were deemed to measure the same underlying construct, a correlation matrix that was factorable needed to include sizable values for the correlation (Field, 2005; Tabachnick & Fidell, 2007).

The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity are generally applied to determine the factorability of such a matrix (Pallant, 2005). The strength of the inter-correlations among the variables within each construct was supported by the inspection of the correlation matrix with evidence of coefficients greater than 0.30. As presented in Table 7, the values of Kaiser-Meyer- Olkin (KMO) of constructs was 0.932 making them well above the minimum acceptable level of 0.60 (Tabachnick & Fidell, 2007). Finally, Bartlett's test of sphericity for each construct was highly significant at $p < 0.001$ level, indicating that there were adequate relationships between the variables included in the analysis (Field, 2005).

Construct	KMO	Bartlett's Test of Sphericity		
Factor Influence Security Culture and Factors Constitutes Security Culture	.932	Approx. Chi-Square	df	Sig.
		4241.558	378	.000

Table 7. KMO and Bartlett's test of sphericity

Then, the Varimax orthogonal rotation was the preferred method, since it was the simplest and most commonly used rotation (Tabachnick & Fidell, 2007). A specific criterion was employed to justify the significance of the factor loadings after the factor had been rotated. A factor loading of 0.50 and above was considered significant at the 0.05 level to obtain a power level of 80% with a sample of 254 (Hair et al., 2006; Tabachnick & Fidell, 2007). Considering the above criteria, table 8 detailed procedures of the EFA for each individual construct (after suppressing loadings of less than 0.4).

Variable	Component				
	1	2	3	4	5
TPM1			.818		
TPM2			.815		
TPM3			.781		
TPM4			.678		
TPM5			.549		
PE1		.507			
PE2		.646			
PE3		.679			
PE4		.665			
T1				.712	
T2				.668	
T3				.776	
AW1	.726				
AW2	.718				

AW3	.745				
AW4	.691				
OWN1					.803
OWN2					.792
OWN3					.781
Eigen value	12.046	3.149	1.533	1.341	1.017
% Variance	43.02	11.245	5.474	4.788	3.632
Cumulative Variance explained	43.03	54.268	59.74	64.53	68.12

Table 8. Rotated factor loadings of the Research Model Constructs

To strengthen the EFA results, CFA was employed to further refine and support the identified factor structures. This process involved assessing how well the factor structure of each construct fitted the data and examining the model parameters to assess construct validity. These factors were treated as a CFA model so that they could portray a set of relationships showing how the measured variables represented a latent factor (Hair et al., 2006). Assessing construct validity using the CFA involved an examination of convergent validity and discriminant validity.

The CFA was performed on each construct using the AMOS (version 18.0) program. The covariance matrix was automatically used as an input data set as a default in AMOS (Shah & Goldstein, 2006). The results are presented in Tables 9 and 10. The factor loading, critical value and significance level of each variable shown in the tables provided a measure for the convergent validity; the value of R^2 provided a measure with which to assess the reliability of the variables; and the value of the correlation between the factors provided an indication of the discriminant validity.

The CFA results of the factors that influence the security culture construct are presented in Table 9. The model appears to have an adequate fit: $X^2 = 94.5$; df = 41; $X^2/df = 2.305$; GFI = 0.939; AGFI= 0.901, NFI = 0.913, TLI = 0.951, CFI = 0.964; IFI = 0.964; and RMSEA = 0.072. All the factor loadings, ranging from 0.578 to 0.852, were greater than the threshold level of 0.50 and were all significant at $p < 0.001$ level, suggesting convergent validity. Table 10 shows CFA results of the factors constituting or reflecting security culture. The model appears to have a good fit: $X^2 = 31.16$; $df = 13$; $X^2/df = 2.397$; GFI = 0.966; AGFI= 0.926, NFI = 0.973, TLI = 0.971, CFI = 0.984; IFI = 0.984; and RMSEA = 0.074. All the factor loadings, ranging from 0.705 to 0.884, were greater than the threshold level of 0.50 and were all significant at $p < 0.001$ level, suggesting convergent validity. The correlation coefficients between factors, at 0.66, were less than 0.850, thus supporting the discriminant validity of the construct.

Factor/Variable	Factor Loading	CR****	*R*2	Correlations
TPM1	.825	f.p.	.68	TPM-Policy Enforcement :.79
TPM2	.852	15.713	.73	
TPM3	.812	14.717	.66	Policy Enforcement –Training: .70
TPM4	.678	11.589	.46	
TPM5	.657	11.143	.43*	
PE1	.754	f.p.	.57	TPM- Training: .56
PE2	.621	9.561	.39	
PE3	.763	11.888	.58	
PE4	.782	12.184	.61	
T1	.782	f.p.	.61	
T2	.790	12.389	.62	
T3	.835	12.930	.70	

*: Eliminated because did not a good fit with the data, f.p.: Fixed Parameter for Estimation; ****: Critical ratio (CR > 1.96: significant at 0.001 level).

Table 9. CFA Results of Factors Influence Security Culture

Factor/Variable	Factor Loading	CR****	*R*2	Correlations
AW1	.886	f.p.	.785	AWR-OWN: .66
AW2	.879	19.040	.772	
AW3	.854	18.235	.730	

AW4	.755	15.046	.570	
OWN1	.837	f.p.	.700	
OWN2	.756	12.631	.572	
OWN3	.826	13.797	.682	

f.p.: Fixed Parameter for Estimation; ****: Critical ratio (CR > 1.96: significant at 0.001 level).

Table 10. CFA Results of Security Culture

Additionally, all of the composite reliability constructs have values above 0.60. In fact the lowest composite reliability value was .883 according to Table 11 which indicates excellent reliability for the construct research model. Furthermore, the average variance extracted for all constructs was greater than 0.50 with a lowest construct value of .654 according to Table 11. These results indicate that the information security culture measurement model possessed substantial convergent validity. Discriminant validity however was also examined using Fornell and Larcker's (1981) recommended conditions for discriminant validity, such as the square root of average variance explained (AVE) for all constructs should be larger than all other cross-correlations and all AVEs should have values above 0.5. The results are presented in Table 12 and indicate that in no case was any correlation between the constructs greater than the average square root of AVE (the principal diagonal element) and all the AVEs were above the 0.5 threshold as discussed earlier. The AVEs ranged from 0.654 to 0.784. The largest squared correlation between policy enforcement and top management involvement was 0.6648 while the smallest square root of AVE obtained is for policy enforcement with AVE of 0.8087. Thus, the discriminant validity of the scales used was adequate for the information security culture measurement model.

Constructs	Composite Reliability	Average Variance Extracted
Top Management Involvement	.915	.725
Policy Enforcement	.883	.654
Training	.902	.754
Awareness	.9355	.784
Ownership	.9045	.759

Table 11. Composite Reliability and Average Variance Extracted

Constructs	Inter-Construct Correlations				
	TPM	PE	T	AWR	OWN
TPM	**.8514**				
PE	. 6648	**.8087**			
T	.4894	.5805	**.8683**		
AWR	.3757	.4668	.4641	**.8854**	
OWN	.3197	.3658	.4196	.583	**.8712**

Table 12. Discriminant Validity for Factors Influence Security Culture and Factors Constitute Security Culture

5 MODEL TESTING

The nomological validity of our information security measurement model is important and essential to the existing body of knowledge in the information security culture area because of lack of any empirical validated theories in information security culture measurement. Nomological validity reflects the extent to which predictions about constructs and measures are accurate from the perspective of reasonably well-established theoretical models (Straub et al., 1995). This paper was designed to develop and test the nomological (predictive) validity of a measure capturing an information security culture measurement model that includes the identification of the relationship between factors influencing security culture and factors constituting or reflecting security culture. Table 13 presented the measurement model assessment, exhibited an acceptable level of fit (X^2 = 252.939, *df* = 129, X^2/df = 1.961, GFI = 0.903, AGFI = 0.871, NFI= .912, TLI = .946, CFI = 0.955, IFI = .955, RMSEA = .062). Additionally, the model testing nomological validity fitted the data well with CMIN = 356.373, df = 234, P=.000, CMIN/df = 1.5229 < 2. The nomological model posits that

security awareness and security ownership are nomologically related to security culture. There are strong correlations between security culture and security culture reflection factors (Awareness and Ownership) with values of .744 and .588 respectively. Additionally, there is also a strong relationship between factors influencing security culture and top management involvement, policy enforcement and training with values of .604, .865 and .559 respectively. Furthermore, the relationship between factors influencing security culture and factors constituting or reflecting security culture, were positive and significant ($\beta = .652$, $p < .001$), with 43 % variance explained in the factors constituting or reflecting security culture. Hypotheses H1 and H2 are significantly supported at $P < .001$, thus supporting the nomological validity of the proposed security culture research model measures.
To further examine the relationship between the components of factors influence security culture and factors constituted security culture, a correlation analysis was performed-see Table 14. The results indicate that all correlations between factors influencing security culture and factors constituting or reflecting security culture are statistically significant.

Construct/ Factor	Factor Loading	CR****	R2	Correlations
Factors Influence Security Culture				Factors Influence Security Culture- Factors Constitute Security Culture: .652
Top Management Involvement	.777	f.p.	.604	
Policy Enforcements	.930	8.774	.865	
Training	.748	8.386	.559	
Factors Constitute Security Culture				
Security Awareness	.863	f.p.	.744	
Security Ownership	.767	7.281	.588	

f.p.: Fixed Parameter for Estimation; ****: Critical ratio (CR > 1.96: significant at 0.001 level).

Table 13. Measurement Model Results and Hypothesis Testing

	Top Management Involvement	Policy Enforcement	Training	Factors Influence Security Culture
Awareness	.376	.467	.463	.511
Ownership	.320	.369	.418	.431
Security Culture	.395	.477	.498	.535

Correlation is significant at the 0.01 level (2-tailed).

Table 14. Correlations among components of security culture with the factors influence security culture

To ensure a better fit for our information security culture measurement model, we compare our results with the alternative measurement model existing from literature analysis in which did not distinguish the difference between factors influence security culture and factors constitute or reflected security culture. In the alternative model, security culture was composed of several factors such as top management involvement, policy enforcement, training, awareness and ownership. In our information security culture measurement model, there was a clear distinction between factors constituting or reflecting security culture (awareness and ownership) and factors influencing security culture (top management involvement, policy enforcement, and training). We compared our information security culture measurement model labelled as 'Model A' with the alterative information security culture model labelled as 'Model B' in order to examine which model might best explain the data. Model B exhibited an acceptable level of fit (X^2= 301.453, df = 130, X^2/df = 2.391, GFI = .883, AGFI=.846, NFI= .895, TLI = .926, CFI = .937, IFI = .937, RMSEA= .072). The results of the alternative model assessment (Model B) are presented in Table 15.

Construct/ Factor	Factor Loading	CR****	R2
Factors Constitute Security Culture			
Top Management Involvement	.752	f.p.	.566
Policy Enforcements	.876	8.525	.767
Training	.771	8.327	.594
Security Awareness	.642	7.914	.412

Security Ownership	.598	7.125	.358

f.p.: Fixed Parameter for Estimation; ****: Critical ratio (CR > 1.96: significant at 0.001 level).

Table 15. Alternative Measurement Model Results

Table 16 compares the goodness of fit statistics for the information security culture measurement model (Model A) and the alternative model (Model B). As can be seen, 'Model A' has better variable indices than 'Model B'. Additionally, the Chi-square (X^2) values of these models were compared with those of the original measurement model. Theoretically, if the Chi-square difference between the two models is significant, the model exhibiting the better fit indices becomes the preferred model. On the other hand, if the Chi-square difference is not significant, the two models are said to have a comparable fit (i.e. both models explain the data equally well). In this case, the Chi-square difference between the two models (Model A) and (Model B) is significant (48.513) at $p < 0.01$, suggesting that all the model parameters did differ significantly. Additionally, to provide a complementary measure for the analysis, the Akaike Information Criterion (AIC) was provided. According to Kline (2005), the model with the smallest AIC is the preferred choice. In this case, Model A has lower (AIC) values of 336.939 compared to 383.452 in Model B. The results indicated that Model A is a more parsimonious representation. Consequently, Model A was chosen as the final model that best represented the survey data.

Fit Indices	Recommendation value	Model A	Model B
X^2	N/A	252.939	301.453
df	N/A	129	130
ΔX^2	N/A	-	48.513*
X^2/df	< 3:1	1.961	2.319
GFI	> .90	.903	.883
AGFI	> .80	.871	.846
NFI	> .90	.912	.895
TLI	> .90	.946	.926
CFI	> .90	.955	.937
IFI	> .90	.954	.937
RMSEA	< .08	.062	.072
AIC	N/A	336.939	383.452

*: Significant at $p < 0.01$

Table 16. Comparison of Models fit indices

6 CONTRIBUTION AND FUTURE WORK

There are some major contributions for the current paper. First of all, the current paper underpinned or identified what constitute a security culture through an extensive review of the literature and exploratory qualitative interviews. On previous literature such as D'Arcy & Greene, (2009) defined security culture as education/communication and management support for security. D'Arcy & Greene, (2009) has not clearly distinct what constitute security culture and what influence security culture. Therefore, the current paper has clearly made this distinction, in which was dedicated to address what constitutes security culture. This constitution of information security culture will serve as a foundation for an early understanding of information security culture and is considered a very important contribution because of a lack of clear definition and conceptualization. Another contribution is the operationalization information security culture measurement model constructs through a literature review, qualitative interviews and an appropriate 'construction of scales' methodological approach. Future research may include investigating the influence of national and organizational culture on security culture. Additional future work could be replicating the study in different environments with different demographic groups. Finally, another important element that conceptualizes security culture is security compliance that must be considered for creating security culture.

References

Burns, A. C., & Bush, R. F. (1998). *Marketing Research*. New Jersey: Prentice Hall.

Chia, P., Maynard, S., & Ruighaver, A. B. (Eds.). (2003). *"Understanding Organisational Security Culture" in Information Systems: The Challenges of Theory and Practice*. Las Vegas, USA: Information Institute.

D'Arcy, J., & Greene, G. (2009). *The Multifaceted Nature of Security Culture and Its Influence on End User Behavior*. Paper presented at the IFIP TC 8 International Workshop on Information Systems Security Research, Cape Town, South Africa.

Da Veiga, A. (2008). *Cultivating and Assessing Information Security Culture*. University of Pretoria.

Da Veiga., A., & Eloff, J. H. P. (2007). Information security culture – validation of an assessment instrument. *Information Systems Management, 24*, 361–372.

Da Veiga., A., & Eloff, J. H. P. (2009). A framework and assessment instrument for information security culture. *Computer & Security*, 1-12.

Da Veiga., A., Martins, N., & Eloff, J. H. P. (2007). Information security culture – validation of an assessment instrument. *Southern African Business Review, 11*(1), 147-166.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339.

Dhillon, G. (1999). Managing and controlling computer misuse. *Information Management & Computer Security, 7*(4), 171-175.

Dojkovski, S., Lichtenstein., Sharman., & Warren. (2007). *Fostering information security culture in small and medium size enterprises: an interpretive study in Australia.* Paper presented at the Proceedings of the 15th European Conference on Information Systems, University of St. Gallen, St. Gallen, Switzerland.

Eloff, M., M, , & von Solms, S., H. (2000). Information Security management: A Hierarchical Approach for various frameworks. *Computer & Security, 19*(3), 243-256.

Field, A. (2005). *Discovering Statistics using SPSS*. London: SAGE Publications.

Fornell, C., & Larcker, D. (1981). "Evaluating structural equation models with unobservable variables and measurement error". *Marketing Research, 18*, 39-50.

Fourie, L. C. H. (2003). The management of Information Security- A South Africa case study. *South Africa Journal of Business Management 34*(2), 19-29.

Furnell, S., Gennatou, M., & Dowland, P. (2001). *Promoting security awareness and training within small organizations*. Paper presented at the 2nd AISM Workshop.

Gaunt. (2000). Practical Approaches to Creating Security Culture. *International Journal of Medical Informatics, 60*, 151-157.

Gerbing, D., & Anderson, J. (1988). 'An updated paradigm for scale development incorporating unidimensionality and its assessment'. *Marketing Research, 25*(2), 186-192.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate Data Analysis*. Upper Saddle River, N.J: Pearson Prentice Hall.

International Standards Organization ISO/IEC TR 13335-1. (2004). *Information technology Security techniques Management of information and communications technology security Part 1: Concepts and models for information and communications technology security management.*

Kline, R. B. (2005). *Principles and Practice of Structural Equation Modeling* (2nd edn ed.). New York: Guilford Press.

Kluge, W. (1998). Secure e-Health: Managing risks to patient health data. *international journal of medical informatics, 76*, 402–406.

Knapp., K., Marshall, E., Rainer, K., & Ford, N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Knapp., K., Marshall, T., Rainer, R., & Morrow, D. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? . *Information System Security, 16*, 100-108.

Koh, K., Ruighaver, A. B., Maynard, S., & Ahmad, A. (2005). *Security Governance: Its Impact on Security Culture.* Paper presented at the 3rd Australian Information Security Management Conference, Perth, Australia.

Kotulic, A. G., & Clark, J. G. (2004). “Why there aren’t more information security research studies?” *Information & Management, 41*(5), 597-607.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*, 509-520.

Lichtenstein, L., & Swatman, P. (2001). *Effective Management and Policy in e-Business Security.* Paper presented at the 14th Bled Electronic Commerce Conference, Bled, Slovenia.

Lim., J., Ahmad., A., Chang., S., & Maynard., S. (2010). *Embedding Information Security Culture Emerging Concerns and Challenges.* Paper presented at the PACIS.

Martins, A., & Eloff, J. H. P. (2002). *Information Security Culture*. Paper presented at the 17th International Conference on Information Security.

Maynard, S., & Ruighaver, A. B. (2002). *"Evaluating IS Security Policy Development"*. Paper presented at the Third Australian Information Warfare and Security Conference, Perth, Australia.

Moore, G., C,, & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information System Research, 2*(3), 192-222.

Nunnally, J., & Bernstein, I. (1994). *Psychometric Theory*. New York: McGraw-Hill.

OECD. (2003). *Guidelines for the Security of Information Systems and Networks*.

Pallant, J. (2005). *SPSS Survival Manual: A Step by Step Guide to Data Analysis using SPSS for Windows (Version 12)*. Berkshire: Open University Press.

Ramachandran, S., Srinivasan, V. R., & Goles, T. (2004). *Information Security Cultures of Four Professions: A Comparative Study.* Paper presented at the 41st Hawaii International Conference on System, Hawaii, USA.

Recker, J. (2008). *Understanding Process Modelling Grammar Continuance: A study of the Consequences of Represential Capabilites* Unpublished PhD Thesis, Queensland University of Technology, Brisbane, Australia

Schlienger, T., & Teufel, S. (2003). *Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture.* Paper presented at the DEXA Workshops.

Shah, R., & Goldstein, S. (2006). 'Use of structural equation modeling in operations management research: looking back and forward'. *Operations Management, 24*(2), 148-169.

Sherif, M., & Sherif, C. (Eds.). (1967). *Attitudes as the individual’s own categories: The social judgment-involvement approach to attitude and attitude change* (C. W Sherif & M. Sherif, Attitude, ego-involvement, and change, 105-139 ed.). Westport, CT: Greenwood Press.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 18*(1), 31-41.

Straub, Limayem, M., & Karahanna, E. (1995). Measuring System Usage: Implications for IS Theory Testing. *Management Science, 41*(8), 1328-1342.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using Multivariate Statistics.* Boston: Pearson Education, Inc.

Tarimo, C. (2006). *ICT Security Readiness Chechlist for Developing Coutries: A Social-Technical Approach.* Unpublished PhD Thesis, Stockolm University, Royal Institute of Technology.

van Niekerk., J., & von Solms, R. (2005). *A holistic framework for the fostering of an information security sub-culture in organizations.* Paper presented at the 4th Annual ISSA Conference South Africa.

Von Solms, S. (2000). Information Security- The Third Wave? . *Computer & Security, 19*, 615-620.

Von Solms, R., & von Solms, S. (2004). From policies to culture. *Computer & Security, 23*, 275-279.

Von Solms., S., & von Solms, R. (2004). The 10 deadly sins of Information Security Management. *Computer & Security, 23*, 371-376.