# An Information Security Culture Model Validated with Structural Equation Modelling

N. Martins and A. Da Veiga

University of South Africa, PO Box 392, UNISA 0003, South Africa
e-mail: martin@unisa.ac.za; dveiga@unisa.ac.za

## Abstract

Information security culture must be considered as part of the information security programme to direct employee behaviour. Such a culture can contribute to the protection of information and minimise the risk that employee behaviour poses. This paper proposes a theoretical model, i.e. an information security culture model (ISCM) with four mechanisms (i.e. management, policies, awareness and compliance) that potentially influence information security culture positively. ISCM is based on the information security culture assessment (ISCA) questionnaire dimensions that are correlated with the theoretical mechanisms (dimensions). The theoretical model is validated through structural equation modelling (SEM) using empirical data derived from an ISCA assessment. This research produces a sound theoretical information security culture model, which is supported by the empirical study and further confirms the research hypothesis that management, policies, awareness and compliance contribute to an information security-positive culture as represented by the validated model.

## Keywords

Information security culture, theoretical model, empirical model, policies, awareness, management, compliance

## 1. Introduction

An information security-positive culture is an important aspect to address when implementing controls to protect organisational information (Furnell & Clarke, 2012; Furnell & Thomson, 2009; Ruighaver, Maynard, & Chang, 2007; Schlienger & Teufel, 2005). An information security-positive culture is evident when information is processed in a secure manner by employees, at all times, whilst preserving the integrity, availability and confidentiality of information and abiding by privacy requirements. This can suffice only when employees exhibit compliance behaviour in line with regulatory requirements and organisational policies. Employees need to have a positive attitude towards the processing of information in order to exhibit acceptable behaviour, which will become the manner in which information is processed over time that postulates in the culture. Employees will be able to comply only if they are supported by management and if there are adequate processes and technology safeguards in place to facilitate such compliance. A combination of people, process and technology safeguards will, together, aid in inculcating an information security-positive culture. Such a culture can also be referred to as a "healthy" or "strong" information security culture. This culture guides employees to behave in a certain manner, depicts what is important for the organisation to protect information and defines how employees should interact with information and what they should strive for (Plunkett and Attner 1994). If employees have shared beliefs and values around the aforementioned concepts they develop a group sense of how to process information securely, which they can use as reference to direct their own interactions with information (Plunkett and Attner 1994).

However, risk is introduced if the organisational culture is not conducive towards the protection of information. In such a culture, employee behaviour – still considered as one of the main threats to the protection of information (PwC 2014, Ponemon 2013) – could lead to information security incidents and breaches. As such, organisations require guidance to "inculcate" or "develop" a strong information security culture whereby the protection of information becomes "the way things are done" in the organisation. In this research we propose to use an information security culture assessment (ISCA) questionnaire (Da Veiga & Martins, 2015) in a study to confirm the theoretical model by means of an empirical model that can serve as guidance for organisations to influence the information security culture positively.

## 2. Background

There are various mechanisms that influence the development of organisational culture, which is a combination of internal (e.g. organisational processes and tangible assets) and external mechanisms (social system and regulators or competitors) (Plunkett and Attner 1994). It is generally recognised that management plays a significant role in influencing an organisational culture (Johnson & Goetz, 2007). Similarly, employees play a role as they need to accept the culture which is facilitated through training (Plunkett and Attner, 1994), such as induction and annual information security compliance training.

Various researchers have investigated an information security culture and the mechanisms that could potentially influence the culture and behaviour of employees (Schlienger and Teufel 2005; Thomson et al. 2006; Kraemer, Carayon, & Clem, 2009; Ruighaver et al. 2007; Van Niekerk and Von Solms 2010; Furnell and Thompson 2009; Van Niekerk and Von Solms, 2010; Furnell & Rajendran, 2012). Management, policies, awareness and compliance are some of the prominent mechanisms that could potentially influence information security culture – see table 1. For the purposes of this research, individual employee mechanisms such as intrinsic and extrinsic motivation (Padayachee 2012, Furnell & Rajendran, 2012) and mechanisms external to the organisation, for example national culture (Hoffstede 1980), are excluded.

| **Mechanisms influencing information security culture** | **Description** |
|---|---|
| Management (Hu, Dinev, Hart, & Cooke, 2012; Johnson & Goetz, 2007; Knapp, Marshall, Rainer, & Ford, 2006; Wilderom, Van den Berg, & Wiersma, 2012) | Management or leadership in the organisation play a critical role in forming the desired culture. They need to define the organisation's information security strategy and lead by example. |
| Information Security Policies (Vroom and Von Solms 2004, ISF 2000, Boxand Pottas 2013) | Employees' knowledge and perception of information security policy rules and procedures could influence the information security culture positively. The information security policy is a critical cornerstone to direct the information security culture and serve as a foundation to create shared values and beliefs. |
| Awareness and Training (Nosworthy 2000, Thomson et al. 2006, Parsons et al. 2014, Herold 2011, Da Veiga and Martins 2015) | Information security awareness and training is implemented to educate employees to understand the risk to information and the relevant controls to use and abide by. Training and awareness has been proven to have a positive impact on the information security culture over time. |
| Compliance (Parsons et al. 2014) | The workforce's knowledge of information security policy and procedures will have a positive impact on the attitude towards the information security policies and compliance. In an organisation where there is a strong or healthy information security culture one would expect compliance as a visible trait of the culture. |

**Table 1: Factors influencing information security culture**

The following hypotheses are subsequently identified:

H1: Management has a positive and strong influence on policies

H2: Policies have a positive and strong influence on awareness

H3: Awareness has a positive and strong influence on compliance

H4: Management, policies, awareness and compliance contribute to an information security-positive culture as represented by a validated model

Although researchers have investigated what mechanisms could influence the information security culture  there is no empirical research where a validated and reliable information security culture instrument has been deployed to derive data to develop a structural equation model for information security culture.

The information security culture assessment (ISCA) (Da Veiga & Martins, 2015) tool is an example of a validated assessment instrument whereby a survey is conducted in the organisation to measure the level of information security culture. In previous research it has been empirically proven that ISCA can be deployed successfully to monitor and improve the information security culture. There is, though, a need to understand the influence between the various constructs (sub-dimensions) in ISCA in order to understand the critical mechanisms (dimensions) that influence the information security culture positively.

In the next section we propose a conceptual model for information security culture and validate it using empirical data through structural equation modelling (SEM). The objective is to further improve the ISCA by understanding the underlying influences of the constructs in the questionnaire and how it influences the development of an information security-positive culture.

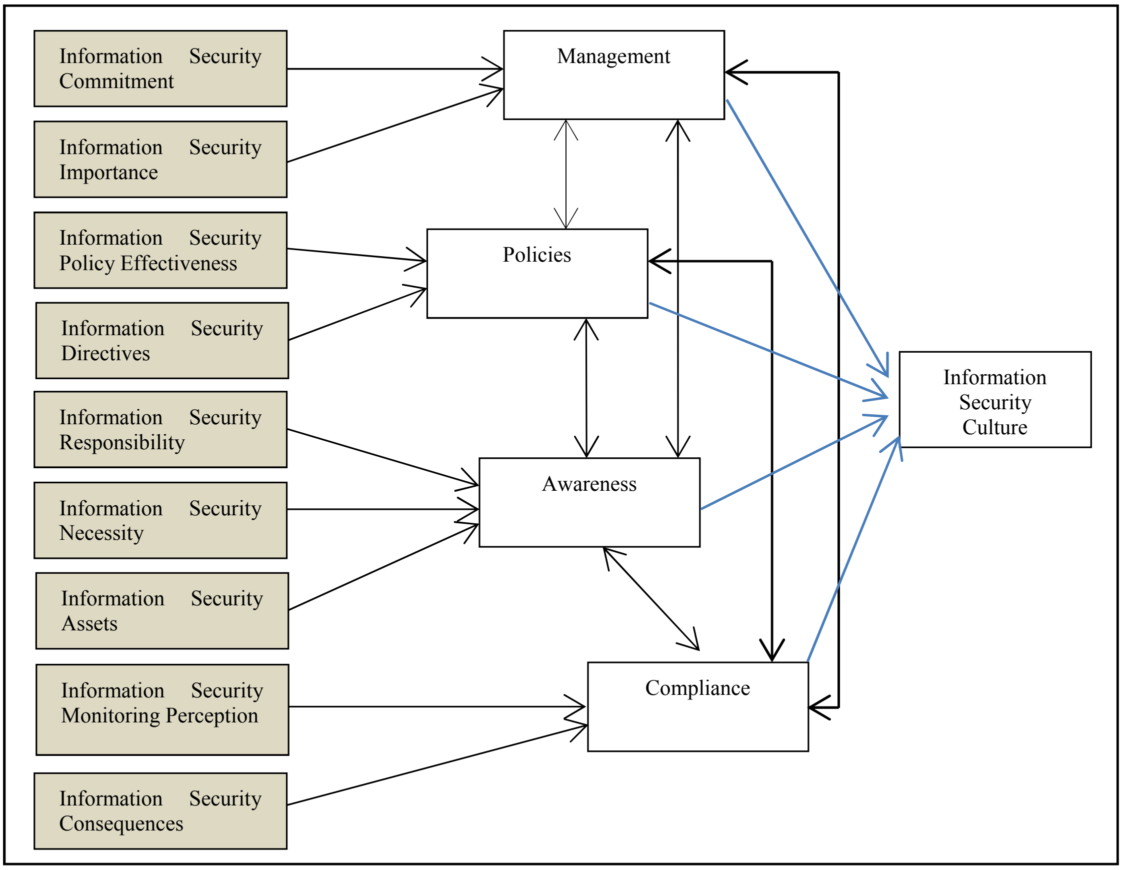

Information Security Commitment
Information Security Importance
Information Security Policy Effectiveness
Information Security Directives
Information Security Responsibility
Information Security Necessity
Information Security Assets
Information Security Monitoring Perception
Information Security Consequences
Management
Policies
Awareness
Compliance
Information Security Culture

**Figure 1: Information Security Culture Model (ISCM)**

## 3. Information Security Culture Model (ISCM)

The constructs of ISCA were used to develop the conceptual Information Security Culture Model (ISCM). The ISCA is comprised of 45 statements across nine constructs. Figure 1 portrays the ISCA constructs that could influence the factors identified in table 1 which, in turn, could influence the information security culture.

The model proposes that the information security culture constructs on the left have a positive influence on the mechanisms, namely management, policies, awareness and compliance. These four mechanisms have a positive influence on each other and in turn have a positive influence on the information security culture. The possible relationships between the constructs will be tested statistically and discussed in the next sections to determine whether the proposed theoretical information security culture model is valid and could influence information security culture.

# 4. Research method and data collection

An ISCA was conducted in 2013 in an international organisation. The convenience sampling method (Brewerton and Millward 2001) was used to distribute the electronic ISCA to the employees. The required sample size for the overall data and biographical areas were calculated using the method of Krejcie and Darryl (1970) which allows for a marginal error of 5% and confidence level of 95%.

Three hundred and seventeen responses were required and 2 159 employees participated, giving a 38,7% response rate from the 8 220 employees. Seventy-six per cent of the participants were non-managerial employees, 20.8% were managers, and 2.4% executives. Only 14.8% worked in IT and the remainder of the respondents in other business functions. Responses were received across 13 business units and 12 countries.

# 5. Data analysis and results

## 5.1. Factor analysis and reliability

To reduce the dimensionality of the data, Principle Axis Factoring (PAF) with IBM SPSS Statistics 22 was used to examine patterns of correlations among the questions used to measure the respondents' perceptions regarding information security.

The factorability of the correlation matrix was investigated using Pearson's product-moment correlation coefficient. Preliminary distribution analyses indicated that the assumptions of normality, linearity and homoscedasticity were not violated. The correlation matrix demonstrated a number of coefficients of 0.3 and above. The Kaiser-Meyer-Olkin value was 0.968, well above the recommended minimum value of 0.6 (Kaiser, 1970, 1974) and the Bartlett's Test of Sphericity (Bartlett, 1954) reached statistical significance, p<.001. Thus, the correlation matrix was deemed factorable.

The ISCA is comprised of questions measuring information security knowledge and culture. The information security culture questions are measured using a 5-point Likert scale, question 19 (Q19) to question 72 (Q72). These 52 questions were initially subjected to PAF and seven of the variables demonstrated very little contribution to the solution with communalities of less than 0.3. These variables were left out of the analysis one by one to see the effect of each. This resulted in a seven-factor solution with two variables (Q47 and Q52) having only loadings of less than 0.3. Thus, it was decided to exclude Q47 and Q52 from the analysis. The remaining 45 variables resulted in a seven-factor solution, explaining 51.42% of the variation in the data.

Due to the large sample, it was decided to allow factor loadings of 0.3 and higher since increasing this cut-of value to 0.4 would result in many more questions that would need to be excluded from the solution. Promax rotation, a rotation method that allows for correlation among the latent factors, was performed. Excluding factor loadings of less than 0.3 resulted in a reasonably simple structure (Thurstone, 1947), with each of the seven factors showing a number of strong loadings, although there are a number of cross-loading situations that need careful interpretation.

Two dimensions were subjected to second-order factor analysis to determine if they could be further analysed. The second-order factor analyses revealed two sub-factors for each of the two dimensions. Each of the extracted factors demonstrates acceptable (or almost) internal consistency as illustrated by the Cronbach's alpha coefficients between 0.909 and 0.545 as shown in table 2. All the values meet the minimum accepted criteria and are above 0.5 (Nunnally & Bernstein, 1994). This analysis confirms the internal consistency and reliability of the ISCA questionnaire.

| **Factors (Constructs)** | **Description** | **Cronbach's Alpha** |
|---|---|---|
| F1 – Information Security Commitment | Commitment from an organisational, divisional and employee perspective regarding the protection of information and implementation controls. | 0.909 |
| F2 – Information Security Importance | The perceived importance of information security by management which includes executives and a divisional perspective. | 0.863 |
| F3 – Information Security Responsibility | Information security responsibility from an end-user perspective. | 0.779 |
| F4 – Information Security Necessity | Information security necessity is established by focusing on specific concepts such as people, time, money and the impact of changes. | 0.847 |
| F5 – Information Security Policy Effectiveness | Assesses the perception of whether the information security policy is understandable and practical and whether it was successfully communicated. | 0.848 |
| F6 – Information Security Monitoring Perception | The perception regarding monitoring and disciplinary action. | 0. 625 |
| F7 – Information Security Assets | Assesses users' perceptions of the protection of information assets in hard copy and electronic format. | 0.915 |
| F8 - Information Security Directives | The perception as to whether the organisation has clear directives for the protection of employee and client information. | 0.888 |
| F9 - Information Security Consequences | Assesses the perception pertaining to recording of and actions taken in the event of non-compliance. | 0. 545 |
| Overall | | 0.849 |

**Table 2: Cronbach's alpha coefficients for the ISCA constructs**

## 5.2. Structural equation modelling (SEM)

SEM has been described as a collection of statistical techniques that allows examination of a set of relationships between one or more independent variables, and one or more dependent variables, either discrete or continuous in both independent and dependent cases (Tabachnick & Fidell, 1983). A confirmatory factor analysis

(CFA) was conducted in order to develop and specify the measurement model (Hair et al., 2010). The AMOS (Analysis of Moment Structures) computer program was used to conduct the CFA. The CFA was conducted using the nine factors identified during the PAF. Once the measurement model has been specified, its validity needs to be determined, which depends on establishing acceptable levels of goodness-of-fit. According to Hair et al. (2010), goodness-of-fit (GOF) indicates how well the specified model reproduces the observed covariance matrix among the indicator items. These results are portrayed in table 3. Except for the chi-square index, all the other GOF indices were at a recommended level (Hair et al., 2010).

| **Indices** | **Value** | **Accepted** |
|---|---|---|
| Chi-square (CMIN) | 4057.386 | No |
| Ratio of CMIN to its degrees of freedom (df) | 792 | Yes, good fit |
| P-value | 0.000 | - |
| Goodness-of-fit index (GFI) | 0.914 | Yes, good fit |
| Root mean square error of approximation (RMSEA) | 0.044 | Yes, good fit |
| Incremental fit index (IFI) - Bollen's IFI | 0.934 | Yes, good fit |
| Tucker Lewis index (TLI) | 0.928 | Yes, good fit |
| Comparative fit index (CFI) | 0.934 | Yes, good fit |

Note: Conventional cut-off: Good fit is indicated by GFI>= .90; TLI, IFI and CFI>= .90 (Garson, 2010)

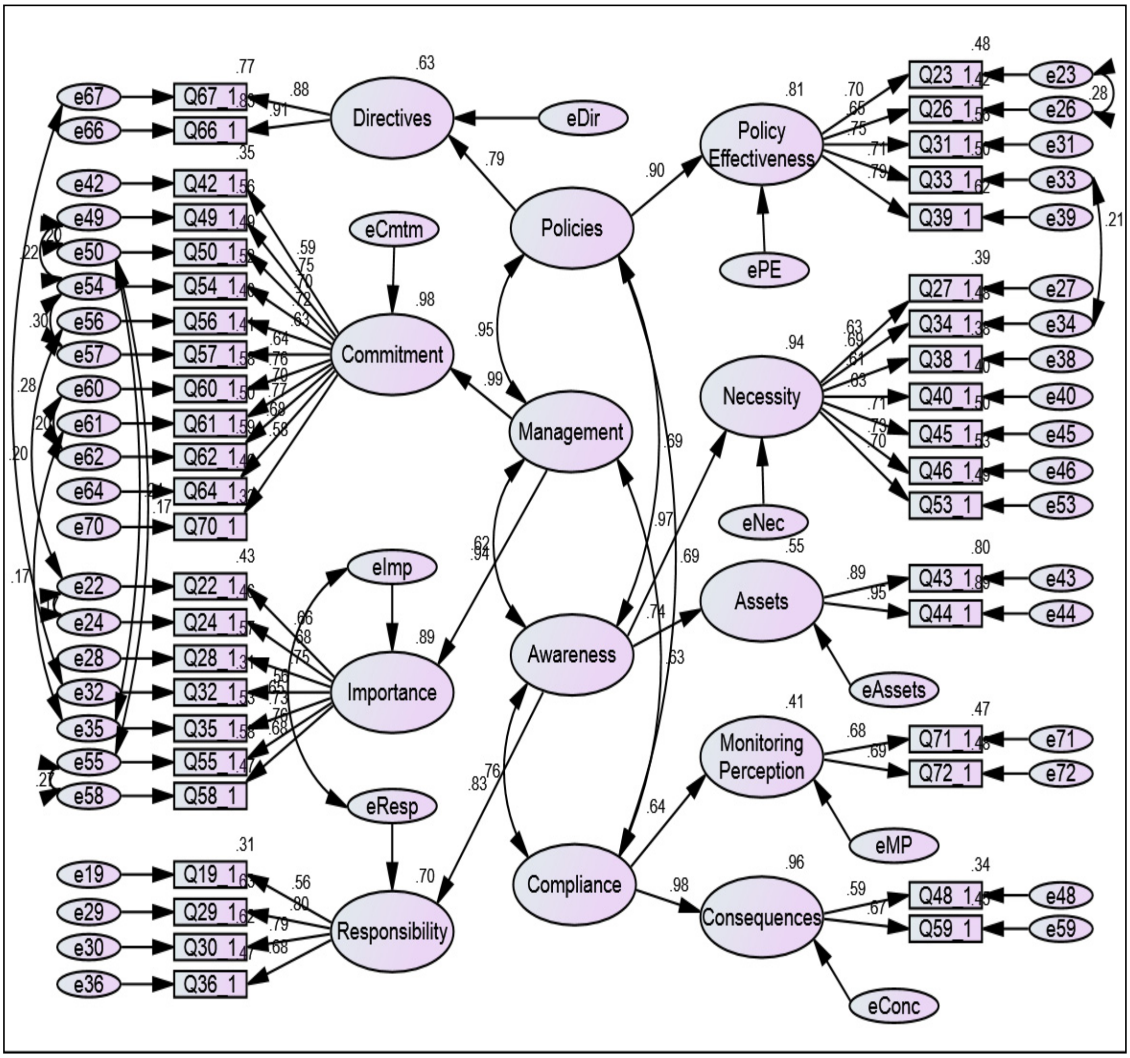
**Table 3: Goodness-of-fit indices for the overall measurement model**

The information security culture structural equation model developed is portrayed in figure 2.

## 6. Discussion

The first hypothesis, namely that management has a positive and strong influence on policies, is confirmed. The second hypothesis, namely that policies have a positive and strong influence on awareness, is also confirmed. The third hypothesis, namely that awareness has a positive and strong influence on compliance, is also confirmed. The last hypothesis, namely that management, policies, awareness and compliance contribute to the measurement of information security culture represented by a validated model, was also confirmed. The results of the SEM provide an indication as to where researchers can focus their information security efforts when they intend to enhance the information security of an organisation by using ISCM.

The results of the SEM model confirm the existence of the four main dimensions (or mechanisms) namely, policies, management, awareness and compliance, (2nd order latent constructs) and nine sub-dimensions (9 ISCA constructs) as depicted in Figure 1. In this model, the focus was on the overall relationships between the different sub- dimensions of the four main dimensions which are in line with the theory and proposed hypothesis. The results of the standardised regression weights, correlations and covariances are all significant. The results of the squared multiple correlations (curved arrows) in figure 2) indicate very high correlations between the main dimensions of management and policies (.95) and awareness and compliance (.76). There are, however, lower correlations between policies and compliance (.63) and management and awareness (.62). This is important for management to take note of as it indicates that management has a high influence on policies and that by focussing on providing adequate direction, and though management support, the information security culture can be positively influenced. Similarly, if employees are aware of information security requirements they will behave in a more compliant manner.



Note: → Regression weights (straight lines), ↶ Correlations (curved lines), 0.00 Squared multiple correlations (figures above the circle)

**Figure 2: Information Security Culture Structural Equation Model (SEM)**

In interpreting the relationship (standardised regression weights as indicated by the straight results on the arrows in figure 2) between the main dimensions and sub-dimensions, most indicate positive to high relationships. The highest relationships are between management and commitment (.99) and importance (.89), policies and policy effectiveness (.90), compliance and consequences (.98). In other words, if management is committed and perceive information security as important they can influence the culture positively. The lowest relationships are between compliance and monitoring perception (.64) and awareness and assets (.63) and necessity (.69). This could indicate that compliance is not necessarily influenced by employees' perception on whether they are comfortable if they are being monitored, thus, they might still exhibit compliance behaviour irrespective of their perception regarding monitoring. Also, employee awareness about the protection of information is not necessarily influenced by distinguishing between hard copy and electronic information. The low relationship between awareness and necessity could indicate that awareness is not necessarily influenced positively through perceptions relating to the necessity of adequate resources to protect information, or employees' views on change, as measured through this dimension. As organisational culture represents a common perception held by the organisation's members (Martins and Martins, 2010) it is important to note that each organisation's culture will differ. This will subsequently have an impact on each organisation's information security culture.

## 7. Conclusion

This research proposed a theoretical information security culture model (ISCM) with the objective of identifying mechanisms that could positively influence the information security culture. The theoretical model was validated using structural equation modelling (SEM) to assist in answering the hypothesis. The research methodology chosen for this research produced a sound theoretical information security culture model which was supported by the empirical study. The exploratory factor analysis produced a reliable factor structure which was confirmed by the SEM confirmatory factor analysis. The SEM methodology enabled the researchers to test and confirm the main dimensions and sub-dimensions influencing information security culture. This ISCM can be used by researchers and organisations to direct their information security initiatives to be in line with the four main dimensions, namely management, policies, awareness and compliance, in order to positively influence information security culture. Their efforts can successfully be monitored by conducting the ISCA survey which will also benchmark data to monitor improvements and developmental areas.

## 8. References

Bartlett, M.S. (1954), "A note on the multiplying factors for various chi square approximations", *Journal of the Royal Statistical Society*, Vol. 16, No. B, pp296 – 298.

Brewerton, P. and Millward, L. (2002), *Organizational research methods*, Sage Publications, London, ISBN 9780761971009.

Box, D. and Pottas, D. (2013)," Improving information security behaviour in the healthcare context", Procedia Technology, Vol. 9, No. 2013, pp1093 – 1103.

Catell, R.B. (1966), "The scree test for the number of factors", *Multivariate Behavioral Research*, Vol.1, pp245 – 276.

Da Veiga, A., and Martins, N. (2015), Improving the information security culture through monitoring and implementation actions illustrated through a case study, *Computers & Security*, Vol. 2015, No. 9, pp162–176.

Furnell, S., and Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. Computers and Security, 31(8), 983–988.

Furnell, S., and Rajendran, A. (2012), "Understanding the influences on information security behaviour", *Computer Fraud and Security*, Vol. 2012, No. March, pp12–15.

Furnell, S., and Thomson, K. L. (2009), "From culture to disobedience: Recognising the varying user acceptance of IT security", *Computer Fraud and Security*, Vol. 2009, No. 3, pp5–10.

Garson, G.D. (2010), "Structural equation modeling example using WinAMOS: the Wheaton study", http://faculty.chass.ncsu.edu/garson/PA765/structur.htm , (Accessed 10 January 2015).

Hair J. F. Jr., Black W. C., Babin B. J., Anderson R. E. And Tatham R. L. (2006). Multivariate data analysis (6th Ed.). Prentice Hall. New Jersey.

Herold, R. (2011), *Managing an information security and privacy awareness and training program*, Taylor and Francis Group, Boca Raton.

Hoffstede, G. (1980), *Culture's consequences: International differences in work-related values*, Sage Publications, Beverley Hills, ISBN 9783423508070.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012), "Managing employee compliance with information security policies : The Critical role of top management and organizational culture ", *Decision Sciences Journal*, Vol. 4, No. 4, pp615–660.

Information Security Forum (ISF). *Information security culture – A preliminary investigation*. s.l.; 2000.

Johnson, M. E., and Goetz, E. (2007), "Embedding information security into the organization", IEEE Security and Privacy, Vol. 2007, No. 5, 16–24.

Kaiser, H. F., (1970), "A second-generation little Jiffy", *Psychometrica*, Vol. 35, No.4, pp410-415.

Kaiser, H. F., (1974)," An index of factorial simplicity", *Psychometrica*, Vol.39, No.1, pp 31-36.

Knapp, K. J., Marshall, T. E., Rainer, R. K., and Ford, F. N. (2006), "Information security: management's effect on culture and policy", Information Management and Computer Security, Vol. 14, No. 1, pp24–36.

Kraemer, S., Carayon, P., and Clem, J. (2009), "Human and organizational factors in computer and information security: Pathways to vulnerabilities", Computers and Security, Vol. 28, No. 7, 509–520.

Krejcie, R.V., Morgan, D.W. (1970), "Determining sample size for research activities", Educational and Psychological Measurement, Vol. 30, No. 1970, pp607-610.

Martins, N, and Martins, E. C. (2004*). Organisational culture*. In S. P. Robbins, & G. Roodt (Eds.), Organisational behaviour: Global and Southern African perspectives. Cape Town: Pearson Education South Africa.

Nosworthy, J.D. (2000), "Implementing information security in the 21st century – do you have the balancing factors?", Computers and Security, Vol. 19, No. 4, pp337-347.

Nunnally, J. & Bernstein, I.H. (1994). Psychometric theory (3rd ed.). New York: McGraw-Hill.

Padayachee K. (2012), "Taxonomy of compliant information security behaviour", Computers and Security, Vol. 2012, No. 31, pp673-80.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", Computers and Security, Vol. 2014, No. 42, pp165–176.

Plunkett, W.R and Attner, R.F. (1994), *Introduction to management*, fifth edition, International Thomson Publishing, California, ISBN: 0534933211.

Ponemon Institute. (2013), "Cost of data breach study: Global analysis benchmark research sponsored by Symantec", http://www.symantec.com, (Accessed 10 June 2014).

PricewaterhouseCoopers (PwC). (2014), "The global state of information security survey",http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml, (Accessed 10 June 2014).

Ruighaver, A. B., Maynard, S. B., and Chang, S. (2007), "Organisational security culture: Extending the end-user perspective", *Computers and Security*, Vol. 2007, No. 26, pp56–62.

Schlienger, T. and Teufel, S. (2005), "Tool supported management of information security culture: An application to a private bank", in Sasaki, R., Okamoto, E. and Yoshiura, H., (eds) *Security and privacy in the age of ubiquitous computing*, Kluwer, Japan.

Tabachnick, B.G. and Fidell, L.S., (2007), *Using multivariate statistics (5th Ed.)*. Pearson Education, Boston, ISBN: 0205459382

Thomson K., Van Solms R. and Louw L. (2006), "Cultivating an organisational information security culture", *Computer Fraud and Security*, Vol. 2006, No. 10, pp 7-11.

Thurstone, L.L. (1947), *Multiple factor analysis*, University of Chicago Press, Chicago, Libraries Australia ID23945090.

Van Niekerk, J. F., and Von Solms, R. (2010). "Information security culture: A management perspective", *Computers and Security*, Vol. 2010 No. 29, pp. 476–486.

Vroom, C. and Von Solms, R. (2004), "Towards information security behavioural compliance", *Computers and Security*, Vol. 2004, No. 23: 191-198.

Wilderom, C. P. M., Van den Berg, P. T., and Wiersma, U. J. (2012), "A longitudinal study of the effects of charismatic leadership and organizational culture on objective and perceived corporate performance", *Leadership Quarterly*, Vol. 23, No. 5, pp835–848.