# The Value of Using a Validated Information Security Culture Assessment Instrument

**Nico Martins[1] and Adéle da Veiga**
**[1]In the Department of Industrial and Organisational Psychology at the University of South Africa (Unisa), Pretoria, South Africa**
martin@unisa.ac.za
adele.daveiga@vodamail.co.za

**Abstract:** It is crucial to understand the perceptions, attitudes and behaviour of an organisation's employees in order to shape the information security culture into one in which the confidentiality and sensitivity of information are understood and handled accordingly. This can be done by conducting an Information Security Culture Assessment (ISCA). The key objective of ISCA is to reduce the risk that employee behaviour poses to the protection of information and to ultimately inculcate a compliance culture with fewer incidents. This paper report on a case study in which the ISCA measurement instrument was deployed successfully in four assessments over a period of eight years. ISCA was expanded for the last two assessments to incorporate the measurement of the perception towards the protection of personal information and privacy, thereby introducing the definition of an information protection culture. A factor and reliability analysis is also reported on as part of the research to revalidate the ISCA measurement instrument. The analysis indicated that the ISCA is valid and reliable when grouping the items into the newly identified factors. The statistical analysis of the four assessments indicated significant improvements based on the corrective actions implemented by the Information Security Officer. The means of each of the dimensions in the 2006 assessment improved compared to the 2013 assessment following the implementation of specific training initiatives over a period of time. It was found that employees who attended training were more positive compared to employees who did not receive training and that the overall Information Security Culture means improved from one assessment to the next.

**Keywords:** information security culture, assessment, behaviour, validity, reliability, privacy

## 1. Introduction

The prevention of loss, damage, unauthorised destruction or access to information processed by organisations is an ongoing evolution. Internal and external risks continuously evolve and often result in breaches. In many instances, employee behaviour is the cause of several information security incidents and privacy breaches (Herold 2011).

Employees in organisations often have access to sensitive information such as the social security numbers, credit card numbers or health information of customers or employees. The manner in which employees process and use the information is critical to prevent mistakes, misuse or incorrect disclosure, which could stem from ignorance, fraud or wilful damage. The culture in an organisation should be conducive to the protection of information. A culture is required in which employees comply with the information security policy and handling requirements. This will help to minimise risks from an employee perspective such wrongful disclosure of sensitive information; unlawful usage of information; unauthorised transfer of information to third parties or outside of legal jurisdictions without the required controls; saving sensitive and/or confidential information in unencrypted format on mobile devices; using internet e-mail accounts to e-mail sensitive and/or confidential information; and infrequent back-ups resulting in inaccurate or lost information.

It is crucial to understand the perceptions, attitudes and behaviour of the organisation's employees in order to shape the information security culture into one in which the nature, confidentiality and sensitivity of information is understood and handled accordingly. This can be done by conducting an ISCA, developed in previous research by the authors (Da Veiga and Eloff 2007, Da Veiga and Eloff 2010, Da Veiga, Martins and Eloff 2007). The first objective of ISCA is to reduce the risk that employee behaviour poses to the protection of information and to ultimately inculcate an information protection culture with fewer breaches resulting from an internal perspective. The second objective of ISCA is to help foster a compliance culture in which the processing of information complies with organisational policy and regulatory requirements.

The regulatory and legal requirements for the processing of information are of critical importance when employees handle information, specifically personal information. The terms "privacy" and "data protection" are often used to refer to the appropriate management of personal information (Swire and Bermann 2007). It is essential that privacy principles are embedded in the information security culture to aid in meeting compliance and customer expectations when processing information. The ISCA can be utilised to also assess the privacy perceptions of employees to help management protect personal information in line with legal requirements, which in many cases also includes the information security requirements that organisations are required to comply with.

## 2. Aim of this paper

The aim of this paper is to validate the ISCA measurement instrument (questionnaire) and test its reliability. This paper provides an overview of information security culture and introduces the concept of privacy. It discusses a case study in which ISCA was deployed and customised to include privacy concepts.

This allowed the researchers to answer the following research questions:

- Is the ISCA measurement instrument valid and reliable in assessing an organisation's information security culture?
- Does the ISCA produce valid results that can be used for management decisions to improve the protection of information in the organisation?

## 3. What is information security culture?

Schein (1985) defines culture as "a pattern of basic assumptions – invented, discovered, or developed by a given group as it learns to cope with its problems of external adaptation and internal integration – that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems". According to Schein (1985), the core substances of corporate culture are the basic assumptions, attitudes and beliefs of employees, which relate to the nature of people and their behaviour and beliefs. Assumptions are values that become embedded and as such are almost taken for granted. These basic assumptions are non-debatable and non-confrontable (Schein 1985).

Organisational or corporate culture is expressed in collective values, norms and knowledge of organisations. Values relate to the sense that people have of what ought to be. Many values are adopted consciously and guide the actions of employees (Schein 1985). Such norms and values affect the behaviour of employees and are expressed in the form of artefacts and creations. Artefacts are the visible output of a culture, for example, the written or spoken language or the way status is demonstrated (Schein 1985).

In terms of the above, Da Veiga and Eloff (2010) define Information Security Culture as the "attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour evident in artefacts and creations that become part of the way things are done in the organisation to protect its information assets."

## 4. Privacy

The concept of privacy goes back as far as 1948 where human rights were defined in the UN Universal Declaration of Human Rights (UN 1948). In 1970, the US Department of Health, Education and Welfare (today referred to as Department of Health and Human Series) developed the Code of Fair Information Practices (Swire and Berman 2007). The Organisation of Economic Cooperation and Development (OECD) published guidelines on the protection of personal information and trans-border flows of personal data in 1980 (OECD 1980) which the US Federal Trade Commission (FTC) endorsed. The USA adopts a sectoral approach to privacy with privacy regulations per industry, for example, the financial or medical sector (Swire and Berman 2007). In Europe, the EU Data Directive 95/46/EC came into effect in 1998, and outlined privacy principles to protect the privacy of individuals and to facilitate the free flow of personal data within the European Union (EU Data Directive 95/46/EC 1995). The EU Privacy Directive is currently being revised to formulate a regulation that will apply to all European member states (APEC 2005). The Asia Pacific Economic Cooperation (APEC) Privacy Framework was established in 2005 (APEC 2005). In Africa alone, there are 15 countries with privacy related laws and five countries in which privacy efforts are under way.

According to Greenleaf (2013), in June 2013, there were 99 countries with privacy laws and about 20 governments in the process of considering such a law. In November 2013, South Africa's Protection of Personal Information Act 2013 (PoPI) was signed into law.

The OECD (1995) privacy principles are enshrined in most of the privacy laws, and focus on the following: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability. Jurisdictions with privacy laws have to comply with regulatory requirements when processing personal information. The security safeguard requirements must be considered throughout the information processing life cycle to preserve the integrity and confidentiality of the information. Organisations need to ensure that their employees are aware of information security and privacy policy requirements which encapsulate regulatory requirements. Employees need to understand the risk to the information they process, implement the required controls to protect it and take accountability for their actions.

An information security culture should be inculcated in which compliance behaviour for all sensitive and confidential information, including personal information, is evident. A culture must be established in which information is protected from risk and the privacy of the information is maintained. As such, ISCA should also incorporate the assessment of employee perceptions towards privacy principles.

## 5. The ISCA methodology

The ISCA methodology comprises an information security culture measuring instrument (questionnaire) and approach developed by the researchers (Da Veiga et al. 2007; Da Veiga and Eloff 2010).

ISCA is used to identify whether there is an acceptable level of information security culture. This means that the level of information security culture provides adequate protection to information assets and thus succeeds in minimising the threat to the confidentiality, integrity and availability of the information asset. The results could indicate that the overall results are positive or that only certain dimensions, statements or biographical groups are positive. If the overall results are positive for certain biographical areas, this means that those employees have a positive perception towards the protection of information, which could mean that there is a good level of awareness, policies are understandable, change is implemented effectively, there is management commitment and training is effective. Having a positive or strong information security culture enables employees to interact with information in a more secure manner, thus creating an environment in which compliance behaviour is the accepted norm and ultimately reduces incidents.

The ISCA methodology (Da Veiga et al 2007) was deployed in the organisation chosen for the case study, to conduct four assessments over a period of eight years. The phases of the methodology include planning, design, survey administration, statistical analysis and reporting. A high-level discussion of the application of ISCA in the case study organisation is provided below.

### 5.1 Planning

The planning phase was used to identify potential stakeholders. A kick-off meeting was held with the project sponsor who, in this case, was the Global Information Security Officer (ISO). During this meeting, a high-level discussion of the information security policy and projects in the organisation took place. Information about training and awareness initiatives in the previous year was also obtained. Relevant information security policies were obtained for background purposes, to customise the ISCA questionnaire. A list of information security awareness topics and training was also obtained in order to incorporate questions about these initiatives. The planning activities were repeated for each of the four assessments. The sample sizes were calculated for each assessment to allow for changes in staff numbers.

### 5.2 Design

The objective of the design phase was to customise the ISCA measurement instrument with the input of the organisation. Eighteen knowledge questions were defined for inclusion in the questionnaire. The purpose of the knowledge questions was to gain an understanding of the employees' awareness of certain information security policy concepts and factors they are expected to know about.

Biographical questions were included to segment the data into 27 regions (including provinces in the breakdown for a total of 12 countries), 13 business units and 3 job levels. An additional question was added to segment the data between employees who had attended information security awareness training, versus those who had not. Another question was added to segment the data between employees working in IT versus other business areas. The objective of the biographical segmentation was to identify any developmental areas across the organisation on which to focus efforts and interventions in order to improve the information security culture.

Forty-four culture questions were included in the questionnaire in line with the previous research (Da Veiga and Eloff 2007; Da Veiga and Eloff 2010). The questions were grouped into 8 dimensions to gauge the perception of employees on the protection of information. The key objective was to identify what perceptions of employees need to change in order to create a culture in which information security is accepted as everyone's responsibility and compliance behaviour becomes evident across the organisation.

Two additional dimensions were added for inclusion in the last two assessments. A dimension focusing on the protection of personal information was added and named, "Privacy Perception". This dimension comprised 9 statements and gauged the perception of certain privacy requirements of employee and customer data in line with the privacy principles of the organisation's privacy policy. A second dimension was added, namely, "Training and Awareness", with two statements to assess specific requirements regarding information security training and to establish the future training needs of employees. Eight additional knowledge questions were added to assess employee perception of the usage and risks relating to personal information. Table 1 outlines the dimensions of the ISCA questionnaire used.

**Table 1:** ISCA questionnaire dimensions

| ISCA dimensions | Description |
|---|---|
| Information Asset Management | Assesses users' perceptions of the protection of information assets |
| Information Security Management | Assesses management's perceptions of information security management |
| Change Management | Assesses the perceptions about change and the willingness of users to change in order to protect information |
| User Management | Assesses user awareness and training with regard to the requirements to protect information |
| Information Security Policies | Assesses whether users understand the information security policy and whether communication thereof was successful |
| Information Security Programme | Assesses the effectiveness of investing in information security resources |
| Trust | Assesses the perceptions of users regarding the safekeeping of private information and their trust in the communications of the organisation |
| Information Security Leadership | Assesses users' perceptions of information security governance (e.g. monitoring) to minimise risks to information |
| Training and Awareness (new) | Assesses employees' perception of additional needs for information security training |
| Privacy Perception (new) | Assesses employees' perception of privacy principles |

Once the Group ISO had approved the ISCA questionnaire, the HTML version was designed and tested. As part of this phase, the communication e-mails and intranet messages that would be used to launch the survey and remind employees to complete the survey by the due date were designed.

### 5.3 Survey administration

This phase includes the survey completion, monitoring and closing out of the survey. The Global ISO sent out the launch e-mail with the survey link as well as the reminder e-mails. A four- to six-week period was provided for employees to complete the survey. The responses received were tracked on a weekly basis to monitor whether enough responses had been obtained in line with the required sample sizes for each biographical area and to motivate employees to respond accordingly.

### 5.4 Statistical analysis

The statistical analysis focused on an overall analysis of the data and comparative analysis for the biographical areas. The data was analysed in means, frequencies and frequency distribution. The SPSS software package (IBM SPSS Statistics 2012) was used for the statistical analysis. Correlation and regression analyses were conducted to determine the most important focuses. Anova and t-tests were used to determine significant differences between the results of the statements for the biographical groupings.

### 5.5 Reporting

During the reporting phase, the statistical analyses were interpreted and developmental areas identified. Once the report had been compiled, a formal feedback session with the Group ISO and relevant stakeholders was conducted.

## 6. Overview of the case study

The case study organisation embarked on a journey to foster a strong Information Security Culture across the organisation. Its objective was to instil a culture in which information security practices would become part of the “way things are done” in the organisation. Under the direction of the Group ISO, four ISCA’s were conducted over a period of eight years, with the first assessment having being done in 2006, followed by another in 2007. In 2010 and 2013 the ISCA was conducted again.

The organisation employed 3 927 employees in 2006, which increased to 8 220 in 2013. The organisation processes financial data on a global basis which is of a sensitive nature and which must be kept confidential from unauthorised parties. In addition, the organisation has to comply with a number of legislative and industry requirements when processing the financial data of organisations and individuals. From a privacy perspective, the data privacy laws in the Australia, Hong Kong, Ireland, Jersey, Mauritius, the UK, the USA and South Africa apply to the organisation. The organisation has established information security policies from an information technology (IT), end user and privacy perspective. The governance of information security across the organisation is affected through country’s ISOs who report to the Group ISO. Generic information security awareness was conducted across the organisation prior to the 2006 ISCA.

### 6.1 Biographical data

In all four assessments, an adequate number of responses were obtained for the overall data analysis:

- 2013 survey: 367 responses were required and 2159 responses were obtained
- 2010 survey: 364 responses were required and 2 320 responses were obtained
- 2007 survey: 351 responses were required and 1571 responses were obtained
- 2006 survey: 351 responses were required and 1941 responses were obtained

This means that the findings could be generalised across the group. The sample size calculation used was based on a marginal error of 5% and confidence level of 95%, to ascertain the findings across the organisation (Krejcie and Morgan, 1970). In 2013, a 38.7% response rate was obtained, 28% in 2010, 29% in 2007 and 40% in 2006. Non-managerial employees represented almost two thirds of the responses in 2013, with the rest being managers. Less than 3% of the respondents were made up of executives.

### 6.2 Overall findings

Table 2 outlines the ISCA dimensions with the corresponding mean and percentage agreement for each dimension for the four assessments. The mean represents the overall mean for a respective dimension comprising a number of statements. The arrows indicate whether the results for a dimension improved (arrow pointing upwards), remained the same (arrow being horisontal) or declined (arrow pointing down wards) from the previous year's assessment. from the previous year's assessment. The results from the 2013 ISCA improved for all dimensions, compared with the 2007 and 2006 data. A cut-off point of the mean of 4.00 was deemed acceptable for the information security assessment, given the importance of information security. This is higher than the 3.37 mean for *The Best Company to Work for* survey.

**Table 2:** ISCA dimension means for 2013, 2010, 2007 and 2006

| ISCA Dimensions | Mean/% Agreement 2013 N = 2 159 | Mean/% Agreement 2010 N = 2 320 | Mean/% Agreement 2007 N = 1 571 | Mean/% Agreement 2006 N = 1 941 |
|---|---|---|---|---|
| Information Asset Management | 4.30, 91.2% ↑ | 4.22, 88.9% ↑ | 4.17, 88.3% ↑ | 4.10, 86.1% |
| Information Security Policies | 4.15, 82.5% ↑ | 4.08, 80.5% ↑ | 4.07, 81.0% ↑ | 3.93, 72.6% |
| Change Management | 4.14, 86.1% ↑ | 4.09, 84.7% ↑ | 4.08, 85.4% ↑ | 3.97, 79.9% |
| User Management | 4.14, 85.8% ↑ | 4.08, 83.4% ↔ | 4.08, 84.9% ↑ | 3.94, 78.8% |
| Information Security Programme | 4.05, 80.55 ↑ | 3.96, 76.8% ↑ | 3.98, 79.9% ↑ | 3.85, 71.0% |
| Information Security Leadership | 4.03, 82.1% ↑ | 3.88, 76.1% ↓ | 3.89, 77.8% ↑ | 3.79, 70.9% |
| Information Security Management | 3.96, 80.1% ↓ | 4.14 90.6% ↑ | 3.88, 79.4% ↑ | 3.84, 76.7% |
| Trust | 3.95, 76.8% ↑ | 3.88, 74.8% ↑ | 3.87, 76.3% ↑ | 3.73, 68.6% |
| Training and Awareness | 3.08, 43.0% ↑ | 3.02, 39.9% ↑ | - | - |
| Privacy Perception | 3.67, 65.4% ↑ | 3.56, 61.5% ↑ | - | - |

It is critical to note in Table 3 that employees who had attended prior information security training were more positive compared to employees who had not attended prior training. The percentage of employees who had received training improved from 2006 by 23.75% to 72.8% in 2013. However, 61.0% of employees indicated in the 2013 survey that they believed there is a need for additional information security training to use information security controls in order to protect information. The awareness initiatives seemed to be effective with 69.4% of employees agreeing with the statements.

**Table 3:** Information security (IS) training means for 2013, 2010, 2007 and 2006

| Mean for training versus no training | 2013 | 2010 | 2007 | 2006 |
|---|---|---|---|---|
| Prior IS training | 4.15 | 3.79 | 4.07 | 4.09 |
| No IS training | 3.96 | 3.65 | 3.92 | 3.83 |

Less than half of the respondents indicated that the organisation's client data was complete and accurate, with only half of the respondents who believed their colleagues ensure that client information is protected when taken off site. Both these views improved significantly from the 2010 to the 2013 surveys. From a privacy perspective, most employees indicated that the organisation has clear directives on how to protect sensitive/confidential client and employee information. Employees also perceived the limitation of the collection and sharing of sensitive, personal information as important.

In summary, it was found that employees believe that they have a responsibility to protect the organisation's information and that information security is necessary in their divisions. It was found that employees are aware of the information security policy and believe that it is applicable to them in their daily duties.

Most respondents indicated that they are willing to accept some inconvenience to secure important information and that they are prepared to change their working practices in order to ensure the security of information assets. There was also a positive perception among respondents that executive and senior management demonstrate commitment to information security. Interestingly, the most preferred method to receive information security communication was through face-to-face presentations, followed by web-based training and e-mail. Another interesting finding was that IT workers were significantly more positive compared to non-IT workers about the culture dimensions, but there were no significant differences for the Privacy Perception and Training and Awareness dimensions**.**

## 6.3 Validity analysis

To determine the factorability and the sampling adequacy, the Kaiser-Meyer-Olkin measure of sampling adequacy and Bartlett's test of sphericity were first conducted. Both the indicators provided adequate scores. Principal axis factoring (PCA) was postulated and the factor matrix obtained was rotated to a simple structure by means of a varimax rotation (Brewerton and Millward 2001, Howell 1995). The scree plot was used to determine the number of factors that should be included in the measurement. From the use of the Kaiser criterion, it emerged that nine factors could be extracted, explaining 54.3% of the total variance based on the cumulative percentage of eigen values. Statements with a value greater than 0.3 were retained and could be regarded as meaningful to be included in a dimension (Hintze 1995). Table 4 indicates the factors with the number of statements grouped into the newly identified factors (dimensions) as well as the statement numbers.

**Table 4** Results of the first factor analysis

| Factors | Number of statements/items | Statements |
|---|---|---|
| Factor 1 | 20 | 49, 55, 50, 54, 62, 35, 61, 58, 57, 28, 60, 22, 56, 24, 66, 64, 42, 21, 47, 32 |
| Factor 2 | 13 | 44, 43, 30, 36, 45, 29, 34, 38, 46, 53, 19, 27, 52 |
| Factor 3 | 5 | 26, 23, 39, 31, 33 |
| Factor 4 | 6 | 48, 63, 40, 20, 59, 41, |
| Factor 5 | 5 | 69, 65, 70, 67, 68 |
| Factor 6 | 2 | 71, 72 |
| Factor 7 | 3 | 25, 37, 51 |

A second-phase factor analysis was conducted to establish whether the items in factor 1 could be further grouped into subdimensions. The analysis indicated that the items could be grouped into two new dimensions as outlined in Table 5.

**Table 5:** Second phase factor analysis – Factor 1

| Factors | Number of statements/ items | Statements |
|---|---|---|
| Factor 1 | 12 | 54, 60, 64, 57, 49, 62, 61, 66, 50, 56, 42, 47 |
| Factor 2 | 8 | 21, 28, 24, 22, 55, 35, 32, 58 |

## 6.4 Reliability analysis

The Cronbach alpha was calculated to determine the reliability of each factor (Church and Waclawski 1998). Table 6 indicates the final six factors (dimensions) of ISCA with the corresponding Cronbach alpa and dimension description. The results indicate that the Cronbach alpa for factor 4 can be improved to 0.930 if statements 23 and 39 are omitted. These statements, however, relate to the measurement of the effectiveness of information security communication efforts. Owing to the importance of assessing the communication efforts, the statements were included. The Cronbach alpha for all six factors was above 0.7, which was deemed acceptable as a minimum value (Brewerton and Millward 2001).

**Table 6:** New ISCA dimensions

| Factor – ISCA dimension | Cronbach alpha | Name | Description |
|---|---|---|---|
| Factor 1 | 0.887 | Information Security Commitment | The perception on the commitment from an organisational, divisional and employee perspective regarding the protection of information and implementation of information security controls. |

| Factor – ISCA dimension | Cronbach alpha | Name | Description |
|---|---|---|---|
| Factor 2 | 0.766 | Management Buy-in | The perception on management buy-in towards information security and the importance attached to the concept by senior managers and executives. The concept of management adherence to the information security policy is also established. |
| Factor 3 | 0.878 | Information Security Necessity and Importance | Information security necessity is established by focusing on specific concepts such as people, time, money and the impact of changes. |
| Factor 4 | 0.798 | Information Security Policy Effectiveness | The effectiveness of the information security policy and the communication thereof is established. |
| Factor 5 | 0.803 | Information Security Accountability | Individual accountability to compliance and the requirements for information security training. |
| Factor 6 | 0.764 | Information Usage Perception | The perception on information security and privacy usage requirements. |

## 7. Conclusion and recommendations

The aim of this research was to conduct an information security culture assessment and to revalidate the ISCA. The results of the statistical analysis, and improvements in the survey instrument and, subsequent interventions after each assessment, illustrated the benefit of utilising the ISCA. The means of each of the dimensions in the 2006 assessment improved compared to the 2013 assessment, following the implementation of specific training initiatives over a period of time. It was found that employees who had attended training were more positive compared to employees who had not received training.

The results also indicated that the ISCA is a valid measurement instrument. The Cronbach alpha showed that the internal consistency of each factor was above the minimum required values, thus contributing to the reliability of the ISCA.

Through this research study, the ISCA was expanded to include privacy concepts. This allows organisations to measure the concept of information security culture in relation to the protection and usage of personal information to effect compliance behaviour. By introducing the concept of privacy it becomes necessary to extend the definition of information security culture and to formulate a definition for this concept. Considering the definition of information security culture and the concept of privacy, an "Information Protection Culture" can be defined by the researchers as "*a culture in which the protection of information and upholding of privacy are part of the way things are done in an organisation. It is a culture in which employees illustrate attitudes, assumptions, beliefs, values and knowledge that contribute to the protection and privacy of information when processing it at any point in time in the information life cycle, resulting in ethical and compliant behaviour."*

In reviewing the adapted ISCA measurement instrument it was found that it could be further improved in the future by considering more statements relating to the appropriate and secure processing of information in line with privacy regulatory requirements. This would entail that the Information Security Culture Framework (Da Veiga and Eloff 2010) which the ISCA is based would need to be amended to support the Information Protection Culture definition and newly defined ISCA dimensions.

The findings of this research are of particular importance to Information Security, Privacy, Risk, Training and Compliance Officers. The findings provide insight into the survey methodology and assessment instrument that organisations can apply to determine current and potential risks from an employee perspective to the protection of information.

## References

APEC, *vide* Asia Pacific Economic Cooperation.

Asia Pacific Economic Cooperation (APEC) Privacy Framework (2005) [online], www.apec.org/.../ECSG/05_ecsg_privacyframewk.ashx.

Brewerton, P. and Millward, L. (2001) *Organizational Research Methods*. Sage, London.

Church, A.H. and Waclawski, J. (1998) *Organizational Surveys: A Seven Step Approach*, Jossey-Bass, San Francisco.

Da Veiga, A. and Eloff, J.H.P. (2010) "A Framework and Assessment Instrument for Information Security Culture", *Computers and Security*, Vol 29, No. 2010, pp 196-207.

Da Veiga, A. and Eloff, J.H.P. (2007) "An Information Security Governance Framework", *Information Systems Management,* Vol 24, No. 4, pp 361-372.

Da Veiga, A., Martins, N. and Eloff, J.H.P. (2007) "Information Security Culture – validation of an assessment instrument", *Southern African Business Review*, Vol 11, No. 1, pp 146–66.

EU Data Directive 95/48/EC, (1995) [online], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

Greenleaf, G. (2013) "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", *Journal of Law, Information and Science*, 2013 UNSW Law Research Paper No. 2013-40.

Herold, R. (2011) *Managing an Information Security and Privacy Awareness and Training Program*, Taylor and Francis Group, Boca Raton.

Hintze, J.L. (1995) *Number Cruncher Statistical Systems*, version 5.03 5/90. Kaysville, UT, NCSS.

Howell, D.C. (1995) *Fundamental statistics for the behavioral sciences*, 3rd International Standards Organisation, Retrieved online in January 2005 from http://www.iso.ch.

IBM SPSS Statistics (2012) "*SPSS version 21.0 for Microsoft Windows platform*", SPSS Inc, Chicago, IL.

Krejcie, R.V. and Morgan, D.W. (1970) "Determining sample size for research activities". *Educational and Psychological Measurement*, Vol 30, pp 607-610.

Protection of Personal Information Act (2013) [online], http://www.actsonline.co.za.

OECD, *vide* Organisation of Economic Cooperation and Development.

Organisation of Economic Cooperation and Development (1980) [online], http://oecdprivacy.org/.

Schein, E.H. (1985) *Organizational culture and leadership*, Jossey-Bass Publishers, San Francisco.

Swire, P.P. and Berman, S. (2007*) Information Privacy, Official Reference for the Certified Information Privacy Professional*, IAPP, Portsmouth.

UN Universal Declaration of Human Rights (1948) [online], http://www.un.org/en/documents/udhr/.