Accepted Manuscript (Unedited)

Appears in: *Computers & Security*

Adéle da Veiga, Nico Martins, Improving the information security culture through monitoring and implementation actions illustrated through a case study, *Computers & Security*, Volume 49, March 2015, Pages 162-176, http://dx.doi.org/10.1016/j.cose.2014.12.006

Improving the information security culture through monitoring and implementation actions illustrated through a case study

Adéle da Veiga[a] and Nico Martins[b]
[a]College of Science, Engineering and Technology, School of Computing, University of South Africa, PO Box 392, UNISA 0003, South Africa
[b]Department of Industrial and Organisational Psychology, University of South Africa, PO Box 392, UNISA 0003, South Africa

Abstract

The human aspect, together with technology and process controls, needs to be considered as part of an information security programme. Current and former employees are still regarded as one of the root causes of information security incidents. One way of addressing the human aspect is to embed an information security culture where the interaction of employees with information assets contributes to the protection of these assets. In other words, it is critical to improve the information security culture in organisations such that the behaviour of employees is in compliance with information security and related information processing policies and regulatory requirements. This can be achieved by assessing, monitoring and influencing an information security culture. An information security culture can be assessed by using an approach such as an information security culture assessment (ISCA). The empirical data derived from an ISCA can be used to influence the information security culture by focussing on developmental areas, of which awareness and training programmes are a critical facet.

In this paper we discuss a case study of an international financial institution at which ISCA was conducted at four intervals over a period of eight years, across twelve countries. Comparative and multivariate analyses were conducted to establish whether the information security culture improved from one assessment to the next based on the developmental actions implemented. One of the key actions implemented was training and awareness focussing on the critical dimensions identified by ISCA. The information security culture improved from one assessment to the next, with the most positive results in in the fourth assessment.

This research illustrates that the theoretical ISCA tool previously developed can be implemented successfully in organisations to positively influence the information security culture. Empirical evidence is provided supporting the effectiveness of ISCA in the context of identified shortcomings in the organisation's information security culture. In addition, empirical evidence is presented indicating that information security training and awareness is a significant factor in positively influencing an information security culture when applied in the context of ISCA.

Key words: Information security culture, assessment, training, awareness, monitoring, benchmark, comparative analysis, survey, human element

1. Introduction

Information security controls have an impact on organisational processes, technology and the manner in which employees process information. To implement information security practices effectively, organisations must ensure that the culture is conducive to the protection of information. Instilling a culture in which information is governed and protected by all employees at all times in accordance with organisational policy and regulatory requirements is by no means an easy task. 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 are understood, and information is handled accordingly.

The pace at which technology is evolving makes shaping an information security culture difficult. The manner in which employees use new technology, such as cloud computing and mobile devices, to access and process organisational information creates new habits and is often a challenge for IT and information security departments, which need to implement controls to protect the organisation's information. A survey conducted by PricewaterhouseCoopers (2014) found that current employees (31%) and former employees (27%) still contribute to information security incidents. Interestingly, the survey results indicated that the number of actual incidents attributable to employees had risen by 25% since the 2013 survey. Research conducted by the Ponemon Institute (2013) indicated that breaches were attributable to human factors (35%), system glitches (29%) and malicious or criminal attacks (37%). An information security programme should therefore be holistic and cover elements from a human, technology and procedural perspective.

A security awareness and training programme is critical to ensure the success of an information security programme (PricewaterhouseCoopers 2014). However, many organisations do not yet have security awareness and training programmes in place. According to the PricewaterhouseCoopers survey (2014), only 54% of organisations in South America, 63% in Asia Pacific, 55% in Europe and 64% in North America have instituted information security awareness and training programmes. It is questionable how effective the information security awareness and training programmes are, as employees still contribute to information security incidents.

This paper illustrates the application of the information security culture assessment (ISCA) in an empirical study that provided the opportunity to assess the effectiveness of the theoretical ISCA developed during previous research. The impact of information security awareness and training programmes as measured through ISCA is analysed to ascertain whether a focus on these aspects could contribute to instilling a stronger information security culture. A stronger information security culture can significantly improve the protection of information, minimise employee-related risk, and enhance compliance with information security and related policy and regulatory requirements. The content and focus of information security awareness and training programmes are essential to ensure their effectiveness. This can be established by conducting ISCA to tailor the audience groups, content

and focus of awareness and training programmes so that they will positively influence the information security culture. In addition, ISCA can help management to identify other factors that might influence the information security culture, such as trust, leadership or change management, which, together with training and awareness, can have a positive influence on the information security culture.

2. Background

The human issue in the context of the processing of information is as important as technology and procedural controls in the protection of the organisation's information assets. Various researchers have focused on the threat that employee behaviour poses to information assets and the extent to which information security constitutes a human issue where perception, attitude and behaviour aspects need to be considered (Ashenden 2008, Thomson et al. 2006, Herath and Rao 2009, Kraemer et al. 2009, Furnell and Clarke 2012, Furnell and Rajendran 2012, Padayachee 2012, Crossler et al. 2013, Flores et al. 2014).The perception, attitudes and behaviour of employees become part of the organisation's culture, and are manifested in the way employees process information. The manner in which employees process and interact with information could be in compliance with the information security policy, but could also pose a threat to information if controls are circumvented. An information security culture develops where employee perception, attitudes and behaviour either contribute to the protection of information or pose a threat to it.

Information security culture has been studied by a number of researchers. Some have focused on defining an information security culture (Nosworthy 2000, Kuusisto and Ilvonen 2003, Schlienger and Teufel 2002, Furnell and Thompson 2009, Van Niekerk and Von Solms 2010) or developing an improved understanding of the concept (OECD 2005). Various research studies have concentrated on the principles (Zakaria and Gani 2003, OECD 2005) and frameworks (Martins and Eloff 2002, Dojkovski et al. 2007, Ruighaver and Maynard 2006, Van Niekerk and Von Solms 2006) on which an information security culture could be based. A number of research perspectives take organisational cultural levels (Martins and Eloff 2002, Zakaria and Gani 2006, Thomson et al. 2006, Ruighaver and Maynard 2006, Van Niekerk and Von Solms 2006, Da Veiga and Eloff 2010) and organisational behaviour levels (Martins and Eloff 2002, Da Veiga and Eloff 2010) into account when defining information security culture. Others (Martins and Eloff 2002, Schlienger and Teufel 2005, Da Veiga et al. 2007, Da Veiga and Eloff 2010) have conducted in-depth research to define a way in which to cultivate and assess an information security culture. Some researchers have specifically investigated the behaviour of employees and their interaction with information systems (Stanton et al. 2005, Thomson and Von Solms 2005, Albrechtsen and Hovden 2010).

In order to influence employees, various information security controls (e.g. awareness, training and monitoring) and processes (e.g. risk assessments) must be implemented, which will contribute to change the information security culture (Nosworthy 2000, Vroom and Von Solms 2004). In 2003, Von Solms and Von Solms suggested that an information security culture could be cultivated through an

information security policy and that communication and education are fundamental to manifest the policy requirements in employee behaviour. The information security policy, together with awareness, can help to create the desired level of information security culture (Gaunt 2000, Herath and Rao 2009).

Thomson, Von Solms and Louw (2006) proposed the Information Security Shared Tacit Espoused Values (MISSTEV) model. The aim of this model is to create information security obedience, which, they argue, could lead to the cultivation of an information security culture. Van Niekerk and Von Solms (2005) defined an outcomes-based framework for culture change. The framework considered outcomes-based education, organisational learning and corporate culture as means to shape the knowledge and attitude of employees with regard to information security. They furthermore compiled a framework (Van Niekerk and Von Solms 2006) using the organisational culture levels of Schein to better understand information security culture.

Some researchers (Nosworthy 2000, Thomson et al. 2006, Parsons et al. 2010, Herold 2011) have argued that training and awareness help to improve an information security culture and contribute to the protection of information from an employee perspective. According to Rebecca Herold (2011), information security (and privacy) training is one of the most effective methods by which a business can safeguard its information assets. The ISO/IEC 27002:2013 (2013) standard includes awareness, training and education as controls that organisations need to implement as part of the code of practice for information security management. According to ISO/IEC 27002:2013, all employees should receive awareness training and updates relating to the organisational policies and procedures relevant to their job function. Training should, moreover, cover the following: security requirements; legal responsibilities and business controls; the correct use of information processing facilities (e.g. log-on procedure), and the use of software packages and information about the disciplinary process. It should, in addition, be relevant to the employee's role, responsibilities and skill; include information on known threats; and include information on whom to contact for further security advice and the proper channels for reporting information security incidents.

Drevin, Kruger and Steyn (2007) introduced the concept of value-focused assessment of information communication and technology (ICT) security awareness in an academic environment. They used the value-focused assessment methodology to determine information security values, which can be converted to objectives. They argue that "the objectives can serve as a basis for decision making and to guide the planning, shaping and development of ICT security awareness programmes and ultimately to influence the general information security culture in a company." They further argue that awareness programmes are essential to develop and grow a strong ICT security culture.

Studies have also focused on what components an information security awareness programme should consider (Rezgui and Marks 2008, Albrechtsen and Hovden 2010, Parsons et al. 2014) and how messages can be conveyed focussing on personality types (Kajzer et al. 2014); others, by

contrast, have defined awareness models (Kritzinger and Smith 2008) as ultimately instilling corporate information security obedience where the vision of senior management has been realised (Thomson and Von Solms, 2005).

Awareness and training can be used to influence the attitude and perceptions of employees positively with regard to information security (Ashenden and Sasse 2013, Ifinedo 2014). A research report of the Command, Control, Communications and Intelligence Division Defence Science and Technology Organisation of Australia (Parsons et al. 2010) investigated the influences on human factors in the information security environment. The authors of the report argue that one of the most effective countermeasures against human factor threats to information security are security awareness, training and education. It is, however, vital to conduct a needs assessment first to ensure that the awareness programme is successful. They also recommend evaluation of and feedback on the awareness programme to ensure its effectiveness in achieving the desired objectives, of which one would be to instil a strong information security culture.

Da Veiga and Eloff defined and validated ISCA in previous research (Martins 2002, Martins and Eloff 2002, Da Veiga et al. 2007, Da Veiga and Eloff 2007, Da Veiga and Eloff 2010). The ISCA instrument focuses on the human element by providing an approach that can be used to cultivate, assess and monitor an information security culture. The output of ISCA is used to identify what components an organisation needs to enhance or improve the protection of the organisation's information from a human perspective. The objective is to instil a stronger information security culture. This is achieved by monitoring the information security culture using ISCA to assess employee knowledge, attitude, perceptions and behaviour in relation to information security. The results obtained from ISCA can be used to direct human interaction with information assets and thereby minimise the threats that user behaviour poses to the protection of information. ISCA can also be used to identify what awareness and training should be conducted in the organisation to instil a stronger information security culture. The information security culture can be measured over a period of time to benchmark empirical data to establish whether the information security culture has improved from one assessment to the next, and whether the developmental actions influenced the information security culture positively.

These perspectives all suggest that information security training and awareness have a positive effect on information security culture. However, they are not based on empirical data measuring an information security culture to ascertain the influence of information security training and awareness on it. The influence of information security training and awareness on information security culture can be verified by means of empirical data to confirm the theoretical perspectives. Information security culture must be measured and monitored over time using a valid and reliable questionnaire to confirm that the information security culture has indeed been assessed and monitored and to make it possible to draw conclusions on the impact of training and awareness. ISCA is carried out via a valid and reliable information security culture questionnaire, whose application can be tested and the effectiveness verified. At the same time the data can be analysed to identify any correlations with

information security training and awareness to support the research perspectives from an empirical point of view.

3. The aim of this paper

This paper discusses a case study of an international financial institution where ISCA was conducted at four intervals (i.e. four assessments) over a period of eight years across twelve countries to establish the effectiveness and practicality of the application of ISCA. ISCA was utilised as part of an organisational project to establish what level of information security culture is present in the organisation, to identify improvements, to benchmark the data from one assessment to the next so as to monitor changes, to identify trends, and to continuously improve the information security culture so as to minimise risk from an employee perspective.

In this paper we intend to illustrate how ISCA was applied to assess the information security culture in the organisation. The empirical study aims to illustrate how an information security culture improves if it is monitored and if aspects identified through ISCA are considered. The study reported on provided empirical evidence of the significant influence that focused training and awareness have over a period of time in instilling a stronger information security culture.

This paper portrays the key findings, trends and recommendations emanating from ISCA by considering the results of the benchmarking data and the following research questions:

- Does the implementation of the recommendations of each ISCA assessment result in an improved information security culture?
- Does information security training positively influence the level of the information security culture?

4. What is an 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, their behaviour and beliefs. Assumptions are values that become embedded and, as a result, are almost taken for granted. These basic assumptions are non-debatable and non-confrontable.

Organisational or corporate culture is expressed in the collective values, norms and knowledge of organisations. Values relate to people’s sense of how things 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, written or spoken language, or the way status is demonstrated (Schein 1985).

Information security culture refers to the shared values ("what is important") and beliefs ("about how things work") that people in the organisation share with regard to information security. It interacts with the organisation's systems and procedures to influence behaviour ("the way we do things around here") (ISF 2000). Information security culture has three focus areas, namely, artefacts and creations; collective values, norms and knowledge; and basic assumptions and beliefs (Schlienger and Teufel 2002).

An information security culture consists of the manner in which employees perceive and interact (behave) with the controls that are implemented to protect information. An information security culture therefore comprises the following:

- basic assumptions regarding information security and how to protect and interact with information in all formats;
- the attitudes and beliefs of employees in respect of information security, controls, compliance and how to protect and interact with information; and
- knowledge of the organisation's information security policy and compliance requirements, what information security incidents are, how to minimise risk to information when processing it, and what constitutes confidential or sensitive information from an organisational as well as a legislative perspective – to mention but a few aspects.

In addition, information security culture relates to the following:

- the values and norms dictating what should be done to protect information and how to handle it in accordance with its sensitivity and classification; and
- visible artefacts and creations of the culture such as clear desks, computers locked with security cables, lockable bins or shredders for the destruction of confidential documents, escorted visitors, encrypted confidential e-mails, annual online information security training, and statistics of the number of incidents related to employee error or negligence.

Given 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."

5. Assessing the information security culture

The verb “assess” means “to estimate the value or quality of” (Oxford 1983, 2005). “Assessing” in the context of ISCA refers to identifying whether the level of information security culture is adequate to protect the confidentiality, integrity and availability of information from an employee perspective. Determining whether the information security culture is at an adequate level requires that a value be determined for it. As part of the research reported on in this paper, this value was determined through a quantitative assessment; this method has been used successfully by researchers in the past (Straub 1990, ISF 2000, Straub et al. 2004, Schlienger and Teufel 2005, Siponen et al. 2007).

Questionnaires and surveys are research tools widely used within the social sciences (Brewerton and Millward 2002) to measure behavioural content pertaining to attitude and opinions (Berry and Houston 1993). To assess the information security culture in an organisation, the attitude and opinions of employees regarding information security need to be determined (Krejcie and Morgan 1970). Through such an assessment, management can measure employees’ perception of information security and identify aspects that require attention so as to improve the information security culture to an acceptable level and in that way protect information.

ISCA involves an information security culture questionnaire developed by the researchers Da Veiga et al. (2007), and Da Veiga and Eloff (2010). The focus of the research reported on here was on assessing employees’ perspectives and knowledge pertaining to the protection of information. A high-level assessment of artefacts was included in the assessment methodology for a holistic assessment of the information security culture output, but this paper does not extend to a discussion of the actual measurement of artefacts.

ISCA is used to identify whether there is an acceptable level of information security culture. This means that the information security culture has to provide adequate protection of information, thus minimising the threat to its confidentiality, integrity and availability. The overall results may be positive, or alternatively only certain dimensions, statements, or biographical groups may display positive results. From an assessment perspective, this would mean that employees selected the “strongly agree” or “agree” option for the statements/questions asked in the questionnaire, utilising a 5-point Likert scale. If the overall results are positive for certain biographical areas, it means that employee perceptions regarding the protection of information are positive, which could indicate an acceptable level of awareness, that information security policies are understandable, that change is implemented effectively, that there is management commitment, and that training is effective. A positive or strong information security culture enables employees to interact with information in a more secure manner, creates an environment where compliance behaviour is the accepted norm, and ultimately reduces information security incidents.

A negative or weak information security culture could result in employees not interacting with information in a secure manner. For instance, employees might find nothing wrong in sharing

passwords, or might value meeting customer expectations above compliance with policies. Employees might not exhibit compliance behaviour. For example, they might not encrypt sensitive transfers of information, or not comply with a clear desk policy. This means that although there might be adequate technology and processes in place, employees might circumvent controls because of their perception of or attitude towards the information security policy requirements. This could stem from the manner in which the organisation introduces the requirements to employees. The information security policy might not be understandable, communication might not be clear or consistent, employees might not be involved in change, management might not set the appropriate example, or there could be a lack of resources such as shredders or lockable cabinets.

The output of ISCA can be used to update information security policies; to provide input for awareness and training programmes, the information security strategy programme and change management programmes; and to guide the focus of external audits. This aids in establishing a structured approach to transforming teams, individuals and the entire organisation to handle information in line with the organisation's information security policies.

6. The research methodology

Quantitative research was conducted in the form of a case study in which ISCA was conducted at four intervals over a period of eight years. The phases of the research methodology include planning, design, survey administration, statistical analysis and reporting. A comprehensive discussion of the application of the research methodology in the case study follows with reference to the research methods used.

6.1 Planning

The case study organisation embarked on a journey to foster a strong information security culture across the organisation. Their objective was to instil a culture in which information security practices became part of the "way things are done" in the organisation. Under the direction of the Group Information Security Officer (ISO), four ISCAs were conducted over a period of eight years – the first in 2006, followed by another in 2007. In 2010 and 2013 ISCA was conducted again. Each assessment was conducted over a period of four to six weeks.

The organisation employed 3 927 employees in 2006, and by 2013 the staff complement had increased to 8 220. The organisation processes global financial data. These data are of a sensitive nature and must be kept confidential from unauthorised parties. In addition, the organisation has to comply with a number of legislative and industrial requirements when processing the financial data of organisations and individuals. 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 the responsibility of the Country ISOs, who report to the Group ISO.

Generic information security awareness training was conducted across the organisation prior to the 2006 ISCA.

The planning phase was used to identify potential stakeholders. A kick-off meeting was held with the project sponsor, in this case, the Group 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 and 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 in the questionnaire.

The planning activities were repeated for each of the four assessments. In some instances additional questions were added, based on changes in the business pertaining to that year's assessment. As part of the planning phase, a project plan was developed to track the project phases, deadlines and activities. Meetings were also conducted with the Communications Department responsible for communicating the survey to the employees, as well as with the Information Technology Department to arrange access for employees to the survey.

6.2 Design

6.2.1 Measurement instrument

The objective of the design phase was to design or customise the survey questionnaire. The ISCA questionnaire was chosen as the research questionnaire, as it assesses information security culture based on a theoretical information security culture model, and was validated in previous research (Da Veiga et al. 2007, Da Veiga and Eloff 2010). By utilising ISCA again and further customising it, the authors aimed to determine whether it can be used in conjunction with specific interventions to influence the information security culture positively over a period of time.

The ISCA questionnaire was customised with the input of the case study organisation. Customisation was necessary, as the information security maturity level of each organisation varies. For example, one organisation might have an implemented information security policy, all employees might have received related training, and their compliance might be monitored. Another organisation might have a draft information security policy that has yet to be implemented. These aspects need to be considered when customising the ISCA questionnaire, to ensure that all questions/statements are relevant to the organisation's environment.

In the case study organisation, a questionnaire customisation workshop was conducted to develop the knowledge questions and biographical questions, and to adapt the culture questions to the language policy of the organisation. Forty-four culture questions were included in the questionnaire, in

line with the previous information security culture constructs developed (Da Veiga et al. 2007, Da Veiga and Eloff 2010). Responses to the culture questions are measured using a 5-point Likert scale (Strongly Disagree, Disagree, Unsure, Agree, Strongly Agree). The scale indicates the respondents' degree of agreement or disagreement with the statements made in each case (Dillon et al. 1993). The option "Unsure" was included at the request of the organisation concerned. It was imperative to keep the culture questions the same to allow benchmarking.

The final culture questions were grouped in the following eight dimensions (constructs) to gauge the perceptions of employees with regard to the protection of information:

1. Information Asset Management (IAM): Assesses users' perceptions of the protection of information assets.
2. Information Security Management (ISM): Assesses management's perceptions of information security management.
3. Change Management (CHANGE): Assesses the perceptions about change and the willingness of users to change in order to protect information.
4. User Management (USERM): Assesses user awareness and training with regard to the requirements to protect information.
5. Information Security Policies (ISPOLICIES): Assesses whether users understand the information security policy and whether this was successfully communicated.
6. Information Security Programme (ISP): Assesses the effectiveness of investing in information security resources.
7. Trust (TRUST): Assesses the perceptions of users regarding the safekeeping of private information and their trust in the communications of the organisation.
8. Information Security Leadership: Assesses users' perceptions of information security governance (e.g. monitoring) to minimise risks to information.
9. Training and Awareness: Assesses employees' perception of additional needs for information security training. This dimension was added for the 2010 and 2013 surveys.

Eighteen knowledge questions were included, based on the organisation's information security policies, relevant information security projects and awareness initiatives. The knowledge question scales varied, depending on the type of question. For the majority of the knowledge questions, a "Yes/No" response was required. The objective of the knowledge questions was to gauge the awareness of employees regarding certain information security policy concepts and aspects that they were expected to be familiar with. The knowledge questions are used as input into the action plans and to determine specific trends.

Biographical questions were included to segment the data into twenty-seven regions (including provinces in the breakdown for a total of twelve countries), thirteen business units, and three job levels. A single response scale was used for the biographical questions. The biographical section of the questionnaire was updated at each assessment to accommodate the organisation's structural

changes. An additional question was added to segment the data into employees who had attended information security awareness training and those who had not. Another question was added to segment the data into employees working in IT and those working in other business areas. The objective of the biographical segmentation was to identify areas of development across the organisation on which to focus efforts and interventions to improve the information security culture.

6.3 The administration of the survey

The administration phase of the survey included the completion, monitoring and finalisation of the survey. Survey Tracker (2015) software was used to distribute, capture and conduct the survey analysis. The ISCA questionnaire was designed in HTML format using Survey Tracker according to the scientific rules of scales and question types built into the software.

The Group ISO sent out the launch e-mail with the survey link to the electronic HTML survey, as well as the reminder e-mails. To encourage participation, employees had the option to participate in a competition, and in so doing stood a chance to win a prize. As the completion of the questionnaire was anonymous, employees were required to provide their e-mail address at the end of the questionnaire, and this was administered outside of the organisation to protect employees' confidentiality.

On each of the four assessment occasions, employees were given a four- to six-week period to complete the survey. The survey was only open for the agreed weeks during each of the four assessment occasions, and data were thus collected only then.

6.3.1 Sampling and biographical data

The ISCA questionnaire was sent out to all employees in the organisation on each assessment occasion. This method is referred to as convenience sampling (Brewerton and Millward 2001). Cross-section data were collected by analysing different sets of data from different sources at a particular time. On all four assessment occasions, an adequate number of responses was obtained for the overall data analysis:

- 2013 survey: 367 responses were required and 2 159 responses were obtained
- 2010 survey: 364 responses were required and 2 320 responses were obtained
- 2007 survey: 351 responses were required and 1 571 responses were obtained
- 2006 survey: 351 responses were required and 1 941 responses were obtained

This means that the findings could be generalised across the organisation. The calculation of the sample size was based on a marginal error of 5% and a confidence level of 95% to ascertain the findings across the organisation (Krejcie and Morgan 1970). The sample sizes were calculated for each assessment occasion to allow for changes in staff numbers. In 2013 a 38.7% response rate was

obtained, compared with 28% in 2010, 29% in 2007 and 40% in 2006. The responses received were tracked weekly during the survey period to monitor whether enough responses were obtained in line with the required sample sizes for each biographical area and to encourage employees to respond.

Non-managerial employees represented almost two-thirds of the responses in 2013, with the rest being managers. Less than 3% of the respondents were executives. Table 2 shows the percentage of responses received per country for each of the four surveys. The most responses were received from South Africa – Johannesburg, and the United Kingdom – London, where the head offices are situated.

Table 1: Percentage of responses received per country

Countries	**% responses received 2013**	**% responses received 2010**	**% responses received 2007**	**% responses received 2006**
Australia	7.7%	7.7%	9.4%	4.0%
Botswana	0.0%	0.1%	0.0%	0.2%
Guernsey	0.1%	2.5%	4.3%	5.3%
Jersey	0.6%	1.7%	1.7%	3.1%
Hong Kong	0.1%	0.2%	0.0%	0.4%
Ireland	2.6%	2.2%	2.5%	0.1%
Mauritius	0.6%	0.8%	2.0%	0.9%
Namibia	0.1%	0.1%	0.1%	0.2%
South Africa – Johannesburg	27.2%	28.0%	35.0%	43.7%
South Africa – Cape Town	7.5%	6.9%	10.2%	12.0%
South Africa – Durban and Pietermaritzburg	1.3%	3.3%	5.4%	5.8%
South Africa – Pretoria	2.7%	2.4%	3.2%	4.3%
South Africa – Port Elizabeth	1.2%	0.9%	1.3%	1.3%
South Africa – East London and Knysna	0.2%	0.2%	0.1%	0.3%
Switzerland – Geneva	0.0%	0.7%	0.8%	1.1%
Switzerland – Zurich	0.7%	0.8%	0.9%	0.3%
United Kingdom – London	27.8%	26.8%	21.6%	15.4%
United Kingdom – Manchester	0.5%	0.7%	0.5%	0.5%
United Kingdom – Reading	2.9%	0.0%	0.0%	0.0%
United Kingdom – Abingdon	0.0%	1.3%	0.5%	0.0%
United Kingdom – Other	13.7%	0.0%	0.0%	0.0%
United States	0.0%	0.2%	0.1%	0.4%
Other	0.5%	1.4%	0.3%	0.3%
No Response	0.1%	11.2%	0.2%	0.5%

6.4 Statistical analysis

The statistical analyses focused on an overall analysis of the data and a comparative analysis for the biographical areas for the data of the four assessment occasions. The data were analysed and the means, frequencies and frequency distribution determined using Survey Tracker.

The SPSS (2013) software package was used for the advanced statistical analyses. Regression analyses were conducted to determine the most important focuses for the 2013 data. ANOVA and t-tests were used to determine significant differences between the results of the statements for the biographical groupings. The t-test compares the results of two groups to determine whether the differences are significant. These tests were used to determine differences in the comparative analysis of biographical areas (Brewerton and Millward 2002). ANOVA tests are used to compare the results of more than two groups to determine whether the differences are significant.

To further enhance the research methodology, focus groups were used to validate the survey results, concentrating on both positive and developmental results and also obtaining employees' input for recommendations and the development of action plans. The feedback from the focus groups largely correlated with the survey results. The results of the focus groups are not included in this paper. Descriptive and multiple regression analysis were further conducted to understand the impact of training on the information security culture using the 2013 data.

6.4.1 Descriptive statistics

The overall results for the 2013 survey are displayed in Table 2. These results indicate that only two of the dimensions are below the proposed cut-off of 4.00 for the mean. A cut-off point of 4.00 for the mean was deemed acceptable for the information security assessment. This cut-off is used because the consequences of non-compliance with the information security requirements could result in the realisation of risk. If just one employee fails to comply, or is not aware of how to process information securely (preserving the confidentiality, integrity and availability of the information), this could result in realisation of risk.

All constructs reveal significant correlations, but none are above .80, which is an indication of a low degree of multicollinearity. It is important to note that the construct of training indicates significance, but low relationships with the other constructs. This is expected, as this construct does not measure any aspects pertaining to the protection of information.

Table 2: Descriptive statistics and Pearson correlation matrix for dimensions

Constructs	Mean	Std. Dev.	1	2	3	4	5	6	7	8	9
1. CHANGE	4.14	.50160	1	.691**	.714**	.608**	.659**	.713**	.682**	.701**	.397**
2. IAM	4.3	.43102	.691**	1	.686**	.541**	.595**	.702**	.615**	.659**	.369**
3. ISL	4.03	.52609	.714**	.686**	1	.502**	.597**	.754**	.728**	.659**	.379**
4. ISM	3.96	.59973	.608**	.541**	.502**	1	.511**	.604**	.461**	.551**	.435**
5. ISPOLICIES	4.15	.51309	.659**	.595**	.597**	.511**	1	.643**	.609**	.634**	.388**
6. ISP	4.05	.45138	.713**	.702**	.754**	.604**	.643**	1	.647**	.654**	.422**
7. TRUST	3.95	.52646	.682**	.615**	.728**	.461**	.609**	.647**	1	.631**	.346**
8. USERM	4.14	.41272	.701**	.659**	.659**	.551**	.634**	.654**	.631**	1	.389**
9. TRAIN	3.09	.58927	.397**	.369**	.379**	.435**	.338**	.422**	.346**	.389**	1

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

6.4.2 Benchmarking statistics: Dimension means of all four assessment occasions

Table 3 provides a summary of the ISCA dimensions with the corresponding means and percentage agreement for each ISCA dimension of the four assessments. The 2006 data were used as the benchmark to monitor improvement over the eight-year period. The mean represents the overall mean for a specific dimension encompassing a number of statements. The arrows indicate whether the results for a dimension revealed an improvement compared with the previous assessment. The results of the 2013 ISCA improved for all dimensions compared with the 2007 and 2006 data.

Table 3: ISCA dimension means for 2013, 2010, 2007 and 2006

ISCA dimensions	Mean / % agreement 2013	Mean / % agreement 2010	Mean / % agreement 2007	Mean / % agreement 2006
Sample size	2159	2320	1571	1941
1. IAM	4.30, 91.2% ↑	4.22, 88.9% ↑	4.17, 88.3% ↑	4.10, 86.1%
2. ISPOLICIES	4.15, 82.5% ↑	4.08, 80.5% ↑	4.07, 81.0% ↑	3.93, 72.6%
3. CHANGE	4.14, 86.1% ↑	4.09, 84.7% ↑	4.08, 85.4% ↑	3.97, 79.9%
4. USERM	4.14, 85.8% ↑	4.08, 83.4% ↔	4.08, 84.9% ↑	3.94, 78.8%
5. ISP	4.05, 80.5% ↑	3.96, 76.8% ↑	3.98, 79.9% ↑	3.85, 71.0%
6. ISL	4.03, 82.1% ↑	3.88, 76.1% ↓	3.89, 77.8% ↑	3.79, 70.9%
7. ISM	3.96, 80.1% ↓	4.14 90.6% ↑	3.88, 79.4% ↑	3.84, 76.7%

8. TRUST	3.95, 76.8% ⬆	3.88, 74.8% ⬆	3.87, 76.3% ⬆	3.73, 68.6%
9. TRAIN	3.09, 43.05% ⬆	3.02, 39.9%	n/a	n/a

In the 2006 survey only one dimension, information asset management, was above the mean of 4. The most positive dimension in the 2013 ISCA was, again, information asset management, with 91.2% of the respondents having positive perceptions (86.1% in 2006).

The number of positive dimensions since 2006 improved from one to six in 2013. Trust was perceived to be the most negative dimension in 2006. This dimension improved to a mean of 3.95, with 76.8% of respondents reacting favourably, compared with 68.6% in 2006.

The benchmark data for the four assessments indicate that the information security culture improved from one survey to the next, with the most positive results reported in 2013. The overall culture mean improved from 3.89 in 2006 to 4.10 in 2013. This mean excludes the training dimension, which was only added in the 2010 and 2013 surveys. In 2006 the overall average of the assessment was 75.7%, compared with 83.6% in 2013, which indicates an improvement in the level of the information security culture. The results of the training dimensions are discussed in 6.4.4.

6.4.3 Benchmarking statistics: Country means for all four assessment occasions

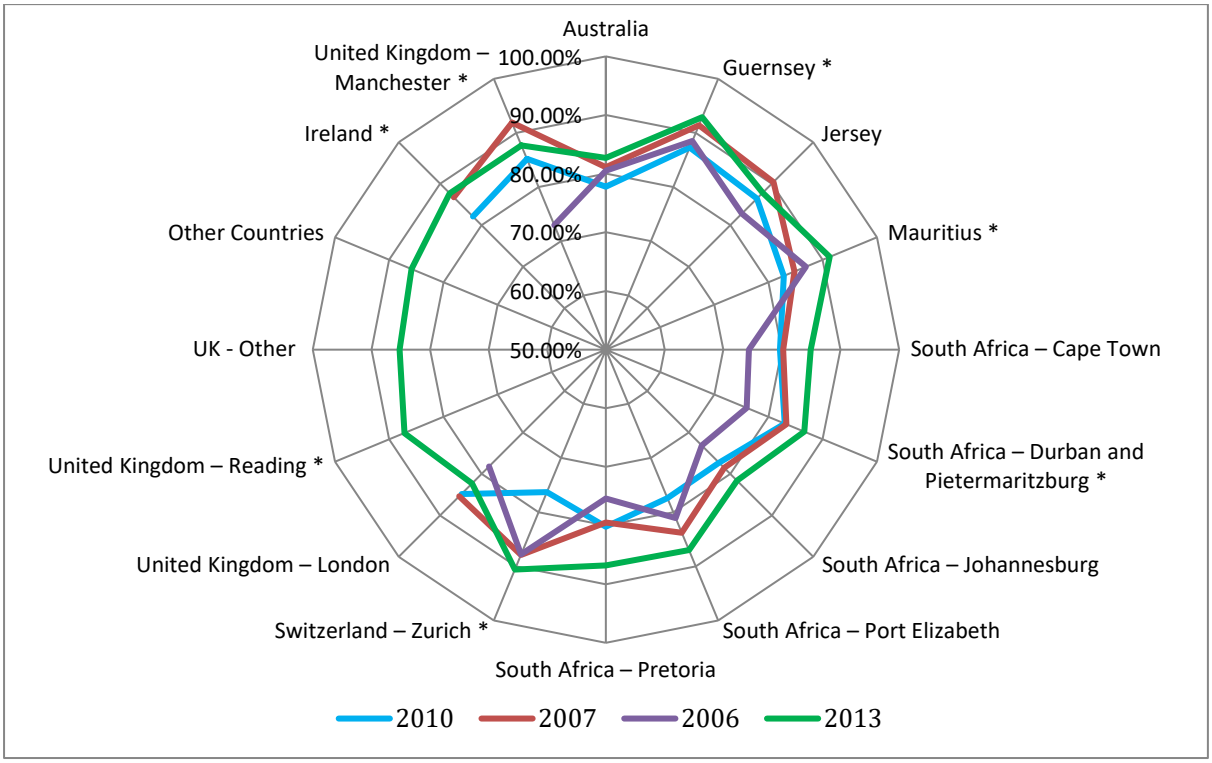
The information security culture improved from one assessment to the next, as is evident in the country comparison of the ISCA averages for the culture statements depicted in Figure 1. The results indicate that the information security culture improved and that employees had a more positive attitude towards information security. Their knowledge about information security improved, and a stronger information security culture was ultimately fostered over time.

The 2013 survey had the most positive results, with the exception of Manchester and Jersey, which were slightly lower in 2013. The countries marked with an asterisk had significantly more positive results in 2013 compared with South Africa – Johannesburg, United Kingdom – London, and Australia. Countries that had fewer than five responses or that were not included in the survey for a specific year owing to structural changes are not included in Figure 1.

The impact of national culture on information security culture in an organisation, which has the potential to contribute either positively or negatively to changing employee behaviour (Martins and Martins 2003), did not form part of the research reported on here. As found by Hofstede (1980) in his cultural research on work related values, the impact of national culture on organisational culture is an

important consideration. As information security culture forms part of organisational culture, the impact should be further researched as part of on-going research.

Figure 1: Percentages for the information security culture section



Note * significantly more positive in 2013

6.4.4 Benchmarking statistics: Training versus no training for all four assessment occasions

Table 4 sets out the percentage of employees who either received or did not receive information security (IS) training in the respective years in which ISCA was carried out. It is clear from the data that the percentage of employees who received information security training increased from 2006 (23.75%) to 2013 (72.8%).

Table 4: Information Security (IS) training received in 2013, 2010, 2007 and 2006

Employees who received prior IS training	2013	2010	2007	2006
Yes	72.8%	66.5%	55.2%	23.75%
No	26.8%	22.4%	44.6%	75.43%
No response	0.4%	11.2%	0.2%	0.82%

The overall information security culture among employees who attended prior information security training was stronger than that among those who did not attend prior training. This is evident in the

data emanating from all four assessments, as depicted in Table 5. A t-test was performed to establish whether the overall information security culture among employees who had received prior training was significantly more positive than that of those who had not. The significance was calculated at a .05 significance level. The results indicate that the information security culture among employees who had received prior information security training was significantly stronger (marked with an asterisk in Table 5) than that among those who had received no such training in 2006 and 2013.

The results relating to the employees who had received prior information security training were more positive in all four years compared with those who had not. The assumption can be made that if employees undergo information security training, they are more aware of the information security policy requirements applicable to them, and their understanding of how to protect information increases. This could contribute to a higher level of compliance and, ultimately, foster a stronger information security culture.

Table 5: Information security (IS) training means for 2013, 2010, 2007 and 2006

Prior training versus no training	**2013 mean**	**2010 mean**	**2007 mean**	**2006 mean**
Prior IS training	4.15*	3.79	4.07	4.09*
No IS training	3.96	3.65	3.92	3.83

Note: * prior IS training significantly better than no prior IS training

Based on the survey findings and other mentioned research dealing with the positive influence information security training has on the information security culture, an additional dimension was added to ISCA specifically to measure information security training requirements. Table 6 shows the two additional statements that were added to the ISCA questionnaire. The percentage of employees who believed that the information security awareness initiatives were successful increased significantly from 2010 (66.1%) to 2013 (69.4%). With 72.8% of employees having received prior information security training and developed greater awareness, the need for training was significantly reduced from 64.9% in 2010 to 61.6% in 2013. Two-thirds of the employees indicated that they believed there is a need for additional training, which emphasises the importance of focusing on information security training.

Table 6: Training and awareness dimension

Training and awareness dimension	**2013 % agree**	**2010 % agree**
I believe the information security awareness initiatives are effective.	69.4% *	66.1%
I believe there is a need for additional training to use information security controls in order to protect Information. **	61.6% *	64.9%

Note: * significant improvement or decline compared with previous year

** Negatively phrased question, results were reversed.

6.4.5 Benchmarking statistics: IT versus non-IT employees on all four assessment occasions

Employees working in IT were significantly more positive compared to employees who did not work in IT, for 2013 (4.15 versus 4.09) and 2006 (3.99 versus 3.88). This may be because employees working in IT are required to implement and monitor the technical information security controls and have a more in-depth understanding of the IT environment. This could be leveraged off to provide support to employees when deploying information security controls. IT employees can participate in forums and discussion groups and training to provide more insight into and guidance on handling organisational information more securely.

6.4.6 Statistical analysis: Statements with significant differences

Statistics were calculated for the 2007, 2010 and 2013 surveys to identify statements in which the overall data improved significantly from one survey to the next. Of the 44 statements, 40 improved significantly in 2007 and 2010, compared with 32 in 2013. This correlates with the overall means, which improved from one survey to the next.

The most positive statements for the four surveys were identified to track the improvements. The means for each of the most positive statements improved from one survey to the next, with the most positive results in 2013. Table 7 indicates five of the most positive statements and the means for each statement for each of the respective years.

Table 7: Comparison of the five most positive statements

Statements	Dimension	Mean 2013	Mean 2010	Mean 2007	Mean 2006
30. I believe I have a responsibility regarding the protection of ABC's information assets (e.g. information and computer resources).	USERM	4.65	* 4.63	4.60	4.57
19. ABC's Information Security Policy is applicable to me during the execution of my daily duties.	ISPOLICIES	* 4.63	* 4.59	* 4.58	4.49
36. Information Security is necessary in my division.	IAM	4.56	* 4.56	4.52	4.41
43. Information assets in electronic media format (e.g. information saved on my hard drive, CDs or a memory stick) need to be protected.	IAM	4.52	* 4.51	* 4.44	4.35
44. Information assets in paper format/hard copy (e.g. contracts, printed reports) need to be protected.	IAM	* 4.53	4.49	* 4.46	4.36

Note: * significant improvement compared with previous assessment

In summary, it was found that employees believed themselves to have a responsibility to protect the organisation's information and that information security was necessary in their divisions. They were aware of the information security policy and believed it to be applicable to them in their daily duties.

Most respondents indicated their willingness to accept some inconvenience in order to secure important information, and their preparedness to change their working practices to ensure the security of information assets. Respondents were of the view that executive and senior management demonstrated commitment to information security. Interestingly, the most preferred method for receiving information security communication was face-to-face presentations, followed by web-based training and e-mail.

6.5 Reporting

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

The developmental areas for countries and business units were identified and specific actions pinpointed for each. Most of the developmental areas for the countries and business units correlated with the overall data, with the exception of a few specific areas. One of those areas was password sharing.

The percentage of employees who reported being aware of colleagues sharing passwords decreased from one survey to the next. As many as 20.6% of the employees in 2006 indicated that they knew of colleagues sharing passwords. This decreased to 13.5% in 2013. Password sharing is still deemed to be a developmental area, with passwords being shared as follows: with helpdesk (9.2%), with managers (2.1%), with secretaries (0.4%) and with colleagues (0.9%).

15.7% of the respondents were aware of an information security incident in their business area in the 12 months preceding the 2013 survey. This reflected a 7.4% increase in the figure revealed by the 2006 survey. A possible reason is that more employees (87.6%) were aware of what constitutes an information security incident compared with the figure revealed by the 2006 survey (72.1%). This could support the assumption that if employees are more aware of what an information security incident is, they will be able to identify and report incidents more effectively.

It could be of value for future research to validate the ISCA results against the actual incidents that were reported and that occurred each year. The expectation is that the actual incidents will be lower if the information security culture is stronger, provided that technical and operational controls are in place. As employees become more aware of what constitutes information security incidents, they may

report more incidents. This would create further awareness, and the culture may change from a reactive culture to a proactive incident prevention culture.

6.5.1 Improving the information security culture at the case study organisation

To improve the information security culture level further, specific topics were identified per biographical area for management to concentrate on during training and awareness sessions, as indicated in the section focusing on the developmental aspects. The Group ISO concentrated on training as the main improvement action in each country, in line with the recommendations of each assessment.

Recommendations pertaining to the information security policy, reporting of incidents and the protection of client information when it is taken off-site were supplied to the organisation, in accordance with data protection regulatory requirements.

Areas in the knowledge section requiring improvement related to:

1. Not knowing the identity of the business unit's ISO
2. Not having read the information security policy
3. Not having received information security communication in the last six months
4. Not knowing where to obtain a copy of the information security policy
5. The belief of some employees that it is permissible to share passwords with the helpdesk, their manager, a secretary or their colleagues

Areas of the culture section requiring improvement related to:

1. Third-party protection of the organisation's information
2. The continuity of the organisation's daily operations in the event of a disaster resulting in the loss of computer systems, people and/or premises
3. Effective communication of the information security policy
4. Timely communication as to how information security changes will affect employees
5. Understanding the content of the information security policy

A multiple regression (stepwise method) analysis (Howell 1995) was performed to determine whether a focus on one variable (e.g. information security management) might improve any aspects of the information security culture. The multiple regression analysis was only conducted for the 2013 data to determine whether training had a significant impact on the information security culture following the training in the previous years and adding the training dimension in the 2010 questionnaire. The results of the multiple regression analysis can be found in Table 8. The strength of the relationship between variables is reflected by the coefficient (Beta value). A high absolute t value and a low

significance value suggest that the predictable variable (dimensions in ISCA) has a significant effect on the dependent variable, namely, the information security management dimension.

To improve information security management still further, a focus on the following dimensions would have the most impact, as indicated in Table 8:

1. Change management
2. Information security programme
3. Training and awareness

The results indicate that a focus on these three dimensions would influence the information security management dimension positively. It is important to note that all three dimensions include aspects of training. This reinforces the value of training as a way to improve information security and, in consequence, the information security culture. The latent value of training and awareness is high, which indicates a small degree of multicollinearity with the other dimensions. The adjustable R Square indicates that the model predicts 47% of the variance in the information security management construct.

The results in Table 8 further indicate that there are negative Beta values for both information security leadership and trust. A possible explanation is that these two constructs focus more on organisation culture than on information security. As indicated in Table 2, the two constructs reveal moderate to high correlations with the other constructs, suggesting that they have an important influence on information security culture.

Table 8: Regression analysis

Dependent variable		Standardised coefficients		Collinearity statistics	
	Constructs	Beta	Sig.	Tolerance	VIF
ISM	(Constant)		.009		
	Change	.268	.000	.323	3.097
	ISP	.266	.000	.318	3.141
	TRAINING	.169	.000	.792	1.263
	USERM	.120	.000	.394	2.539
	ISL	-.093	.001	.301	3.324
	IAM	.086	.001	.391	2.555
	ISPOLICIES	.068	.003	.457	2.188
	TRUST	-.056	.025	.390	2.564

Notes:

1. Dependent variable/constant: information security management dimension.
2. Standardised coefficients (Beta) give a measure of the contribution of each variable. It is the regression coefficient that results from the unstandardised coefficient data that has been standardised to have a mean of 0 and a standard deviation of 1 on each variable.

3. Significance provides an indication of the impact of each variable.
4. The adjustable R Square (R^2) is 47% with a significant change of .025.

7. Discussion

The answer to the first research question, namely: “Does the implementation of the recommendations of each ISCA result in an improved information security culture?” is evident from the improvement in the overall culture means from one assessment to the next, with the most positive results obtained in 2013. The theoretical ISCA developed in previous research is proven to be effective and practically implementable by yielding results over a period of time relating to the improved information security culture, provided the action plans identified in the ISCA are implemented.

The results for the respective dimensions and biographical groups improved from one assessment to the next, with a number of statistically significant improvements at statement level. ISCA serves as an effective tool to conduct a needs assessment or to benchmark the degree to which an information security culture exists in an organisation. The output appears to be effective in identifying specific focus areas such as training and change management that require further development. ISCA is beneficial in identifying specific biographical groups (e.g. job levels, business units, regions or generation groups) that require improvement as well as the specific aspects to focus on for each (e.g. to read the policy, address management commitment, address perception regarding password sharing). Implemented practically, ISCA thus appears to be successful as a tool to achieve the continuous improvement of an information security culture.

The answer to the second research question, namely: “Does information security training positively influence the level of the information security culture?” is to be found in the empirical evidence emanating from the study reported on in this paper. Employees who had received prior information security training responded more positively than those who had not. This was evident in the comparison analysis of the four assessment occasions and the t-tests. The additional training and awareness statements that were added indicated that employees required information security training in order to protect information further. After eight years of information security training and initiatives to improve the information security culture, two-thirds of the employees continued to indicate that they felt additional training to be necessary; this constitutes evidence of the importance of focusing on information security training. The results of ISCA showed that those employees who attended information security training appeared to demonstrate a more positive (shared) information security culture than those who did not.

The regression analysis indicated specific dimensions requiring management’s attention to positively influence the information security culture. The dimensions to focus on will differ from one organisation to the next, as well as from one ISCA to the next in the same organisation. One of the benefits of ISCA is that it makes it possible to identify those aspects that will contribute the most to improving the information security culture. Although training and awareness were found to be critical for the case

study organisation, a number of other factors can also play a role in improving the information security culture.

8. The value of the ISCA questionnaire

The ISCA questionnaire was subsequently administered in a number of organisations in South Africa. The case study organisation was the only organisation to date in which four ISCAs were conducted in order to derive benchmark data for a specific organisation over a period of time in order to ascertain a long-term influence. The organisations that participated in the ISCA assessments used the output of the assessment for various applications. The case study organisation used the ISCA results mainly to tailor and focus awareness and training programmes across business units and countries. It was also used by the Group ISO to update the group information security policies. The empirical data enabled the Group ISO to provide evidence of an improved information security culture and greater information security awareness among employees. This added significant value in demonstrating that the resources deployed to implement action plans were successful across business units and countries. The output of ISCA was also considered in directing internal audit initiatives by identifying high-risk business units, such as those where employees shared passwords or where employees indicated that they did not understand the information security policy.

The ISCA questionnaire is a flexible instrument that can be adapted for various industries, organisational sizes and countries, and different levels of maturity of information security programmes. Where possible, the ISCA dimensions are retained to preserve the content validity of the questionnaire. Additional statements are usually added as separate dimensions, as in the case study organisation, where the training and awareness dimension was added. A project management dimension was added in another ISCA assessment, because the organisation's information security initiatives were driven through formal projects. In all the ISCA assessments, as in the case study organisation, ISCA was used as part of a wider information security programme to address the human aspect together with procedural and technology projects to mitigate risks to information.

Various technologies are available for conducting surveys, allowing for ISCA to be administered in organisations throughout the world. In the case study organisation, Survey Tracker was used as the software for administering the survey. Employees in various countries accessed the survey via the internet. Paper questionnaires are another option that can be considered if not all employees have access to computers. This was, for instance, the case in another organisation that had offices in Africa with limited internet connection. ISCA has also been administered in an organisation that opted to make the questionnaire available to their employees in more than one language, in that case English and French. The organisation provided the translation. These are just a few examples of the scalability of ISCA for use across various industries, locations and organisational sizes.

This is part of ongoing research, and the ISCA questionnaire is improved with each assessment. The customisation of the questionnaire requires that a validity and reliability analysis must be conducted each time ISCA is administered. It will be beneficial if certain statements in ISCA are fixed (i.e. cannot be customised or removed). This will allow industry and country benchmarking between ISCA assessments of different organisations and will also ensure that a valid and reliable questionnaire is used at all times.

9. Conclusion

The objective of ISCA is to help organisations foster an information security culture in which the nature, confidentiality and sensitivity of information are understood, and information is handled accordingly by employees. ISCA aids in identifying the components (leadership, trust, etc.) an organisation needs to enhance or improve the protection of the organisation's information from a human perspective. The output of ISCA provides metrics that can be used to highlight specific focus areas for the organisation to concentrate on, thereby enabling the workforce to align themselves with the organisation’s information security requirements.

The research provides empirical evidence that an information security culture can be influenced positively by using ISCA and implementing the recommendations emanating from the empirical data. The empirical data show that training and awareness have a significant positive impact on the information security culture in an organisation. Many aspects influence an information security culture positively, such as a focus on change management or the information security programme. Naturally, these aspects are different for each organisation, but ISCA aids management in determining where to focus. This helps the organisation to optimise money, resources and time spent on cultivating an acceptable information security culture and to prevent overinvestment in, for instance, business units or countries where the information security culture is already at an acceptable level. ISCA raised awareness in the case study organisation regarding the protection of information, and thus contributed to cultivating an information security culture. Employees who received information security training appeared to have a more positive information security culture (shared culture) than those who did not undergo such training.

In summary, the research illustrates that the level of an organisation’s information security culture can be improved by means of ISCA, and through implementing the proposed recommendations; moreover, the application of ISCA in a range of contexts contributes to the relevance and effectiveness of this instrument. Value is derived by attending to the developmental areas identified by means of ISCA through specific action plans. Focusing on information security training and awareness has a positive influence on the information security culture and enhances the information security culture over a period of time. Through a positive influence on the information security culture, the human element is considered and employee behaviour directed through the corrective actions implemented.

The findings of the research reported on in this paper are of particular importance to ISOs, risk and compliance officers and information security managers. ISCA can aid management in directing and prioritising information security awareness and training, because it highlights the topics and biographical groups in the organisation that require attention. It provides insight into possible approaches that organisations can adopt to reduce the risk to the protection of information from an employee perspective. The trends identified in the case study also indicate how an information security culture is inculcated at an acceptable level in an organisation.

ISCA could be improved in future research by drawing a correlation between the employee perception on reporting incidents and the actual incidents reported. This would help to determine whether fewer incidents occur as the information security culture becomes more entrenched. The ISCA approach can be improved by incorporating linkage research (Wiley and Brooks) to verify whether employees' perceptions, as measured through ISCA, are in line with their compliance behaviour, verified through interventions such as compliance assessments, IT audits and monitoring.

This research paper focused on the impact of training and awareness. However, the data can be analysed further to determine the impact of other factors, and to draw more correlations, such as the impact of reading the information security policy compared to employees who did not. The questionnaire could also be improved by conducting further reliability and validity tests, determining the factorial invariance across countries and considering the impact of national culture. It would also be beneficial to industry to identify fixed questions in the ISCA questionnaire that can be used to benchmark information security culture data across organisations.

10. References

Albrechtsen E., Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security 2010; 29(2010):432–445.

Ashenden D. Information Security management: A human challenge? Information security technical report 2008; 13(2008):195–201.

Ashenden D., Sasse A. CISOs and organisational culture: Their own worst enemy? Computers & Security 2013; 39(2013):396–405.

Berry M.L., Houston J.P. Psychology at work. Wisconsin: Brown and Benchmark Publishers; 1993.

Brewerton P., Millward L. Organizational research methods. London: Sage Publications; 2002.

Crossler R.E., Johnston A.C., Lowry P.B., Hud Q., Warkentin M., Baskerville R. Future directions for behavioral information security. Computers & Security 2013; 32(2013):90–101.

Da Veiga A., Eloff J.H.P. An information security governance framework. Information Systems Management 2007; 24(4):361–372.

Da Veiga A., Eloff J.H.P. A framework and assessment instrument for Information Security Culture. Computers & Security 2010; 29:196–207.

Da Veiga A., Martins N., Eloff J.HP. Information security culture—validation of an assessment instrument. Southern African Business Review 2007; 11(1):147–166.

Dillon W.R., Madden J.T., Firtle, N.H. Essentials of marketing research. Boston: IRWIN; 1993.

Dojkovski S., Lichtenstein S., Warren M.J. Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. ECIS 2007 Proceedings 2007; Paper 120, from http://aisel.aisnet.org/ecis2007/120

Drevin L., Kruger H.A., Steyn T. Value-focused assessment of ICT security awareness in an academic environment. Computers & Security 2007; 26(2007):36–43.

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

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

Furnell S., Rajendran A. Understanding the influences on information security behavior. Computer Fraud and Security 2012; March:12–15.

Furnell S., Thomson K. From culture to disobedience: Recognising the varying user acceptance of IT security, Computer Fraud and Security 2009; Feb 2009:5–10.

Gaunt, N. Practical approaches to creating a security culture. International Journal of Medical Informatics 2000; 60(2):151–157.

Herath T., Rao H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 2009; 47(2009):154–165.

Herold R. Managing an Information Security and Privacy Awareness and Training Program. 2nd ed. Boca Rotan: CRC Press; 2011.

Hofstede G. Culture's Consequences: International Differences in Work-related Values. Beverley Hills: Sage Publications; 1980.

Howell D.C. Fundamental statistics for the behavioral science. 3rd ed. California: Wadsworth Inc; 1995.

IBM SPSS Statistics. SPSS version 21.0 for Microsoft Windows platform. Chicago: SPSS Inc; 2012.

Ifinedo P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management 2014; 51(2014):69–79.

ISF (Information Security Forum). Information Security Culture – A preliminary investigation. s.l; 2000.

ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security management; 2013.

Kajzer M., D'Arcy J., Crowell C.R., Striegel A., Van Bruggen D. An exploratory investigation of message person congruence in information security awareness campaigns. Computers & Security 2014; 43(2014):64–76.

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

Krejcie R.V., Morgan D.W. Determining sample size for research activities. Educational and Psychological Measurement 1970; 30:607–610.

Kritzinger E., Smith E. Information security management: An information security retrieval and awareness model for industry. Computers and Security 2008; 27(2008):224–231.

Kuusisto R., Ilvonen, I. Information security culture in small and medium-sized enterprises. Frontiers of E-business Research, 2003, from http://www.academia.edu/1075891/Information_security_culture_in_small_and_medium_size_enterprises

Martins A. Information security culture, M.Com thesis. Johannesburg: Rand Afrikaans University; 2002.

Martins A., Eloff J.H.P. Information Security Culture. IFIP/SEC2002, in Security in the information society. Boston: Kluwer Academic; 2002:203–214.

Martins N., Martins E. Organisational Culture. In: Robbins S.P., Odendaal A., Roodt G. editors. Organisational Behaviour Global and Southern African Perspectives. Cape Town: Pearson Education South Africa; 2003.

Nosworthy J.D. Implementing information security in the 21st century – do you have the balancing factors? Computers and Security 2000; 19(4):337–347.

OECD (Organisation for Economic Cooperation and Development). The promotion of a culture of security for information systems and networks in OECD countries, 2005, from www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

Oxford. See The Concise Oxford Dictionary.

Padayachee K. Taxonomy of compliant information security behavior. Computers & Security 2012; 31(2012):673–680.

Parsons K., McCormac A., Butavicius M., Ferguson L. Command Human Factors and Information Security: Individual, Culture and Security Environment. Control, Communications and Intelligence Division. Defence Science and Technology Organisation; 2010.

Parsons K., McCormac A., Butavicius M., Pattinson M., Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security 2014; 42(2014):165–176.

Ponemon Institute. Independently Conducted by Ponemon Institute LLC. Cost of Data Breach Study: Global Analysis Benchmark research sponsored by Symantec; 2013, from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013.

PricewaterhouseCoopers (PwC). The Global State of Information Security Survey. 2014, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

Rezgui Y., Marks A. Information security awareness in higher education: An exploratory study. Computers & Security 2008; 27(2008):241–253.

Ruighaver A.B., Maynard S. Organizational Security Culture: More Than Just an End-User Phenomenon. In Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006); Karlstad, Sweden; 2006:425–430.

Schein E.H. Organizational culture and leadership. San Francisco: Jossey-Bass; 1985.

Schlienger T., Teufel S. Information security culture. In Security in the Information Society. IFIP/SEC2002. Kluwer Academic: Boston; 2002:191–201.

Schlienger T., Teufel S. Tool supported management of information security culture, in IFIP International Information Security Conference (20th: 2005: Makuhari-Messe, Chiba). Japan; 2005.

Siponen M., Pahnila S., Mahmood A. Employees' adherence to information security policies: An empirical study, in Proceedings of New Approaches to Security, Privacy and Trust in Complex Environments. Sandton, South Africa : FIP/SEC2007; 2007:133–144.

SPSS version 22. IBM Software Group, ATTN: Licensing, 200 W. Madison St. Chicago, IL; 60606, U.S.A.; 2013.

Stanton J. M., Stama K.R, Mastrangelob P., Joltonb J. Analysis of end user security behaviors. Computers & Security 2005; 24(2005):124–133.

Straub D.W. Effective IS security: an empirical study. Information Systems Research 1990; (1):255–276.

Straub D., Boudreau M., Gefen D. Validation guidelines for IS positivist research, Communications of the Association for Information Systems 2004; 13(24):380–427.

Survey Tracker. Training Technologies Inc. 2014, from https://www.surveytracker.com/

The Concise Oxford Dictionary. Oxford: Clarendon Press; 1983, 2005.

Thomson K., Von Solms, R. Information security obedience: a definition. Computers & Security 2005; 24(1):69–75.

Thomson K., Van Solms R., Louw L. Cultivating an organisational information security culture. Computer Fraud and Security 2006; October: 7–11.

Van Niekerk J., Von Solms R. An holistic framework for the fostering of an information security sub-culture in organizations. In Information Security South Africa – Proceedings of ISSA 2005, 4th Annual Information Security South Africa Conference. South Africa; 2005.

Van Niekerk J., Von Solms R. Information security culture: A management perspective. Computers and Security 2010; 29(2010):476–486.

Van Niekerk J., Von Solms R. Understanding information security culture: A conceptual framework. In Information Security South Africa – Proceedings of ISSA 2006, 5th Annual Information Security South Africa Conference. South Africa; 2006.

Von Solms, R., Von Solms, B. From policies to culture. Computers and Security 2004; 23(2004):275–279.

Vroom C., Von Solms R. Towards information security behavioural compliance. Computers and Security 2004; 23(3):191–198.

Wiley C.P.M., Brooks S.M. The high-performance organizational climate: How workers describe top-performing units. In: Ashkanasy, N.M, Wilderom, C.P.M, Peterson, M.F., editors. Handbook of Organisational Culture and Climate. California: Sage Publications; 2000, p117–192.

Zakaria O., Gani, A. A conceptual checklist of information security culture. In Proceedings of the 2nd European Conference on Information Warfare and Security. Reading, UK; 2003.