Information security culture – validation of an assessment instrument

A. da Veiga, N. Martins & J.H.P. Eloff

ABSTRACT

Organisations need to ensure that the interaction among people, as well as between people and information technology (IT) systems, contributes to the protection of information assets. Organisations therefore need to assess their employees' behaviour and attitudes towards the protection of information assets in order to establish whether employee behaviour is an asset or a threat to the protection of information. One approach that organisations could use is to assess whether an acceptable level of information security culture has been inculcated in the organisation and, if not, take corrective action. The aim of this paper is to validate an information security culture assessment instrument. This is achieved by performing a factor and reliability analysis on the data from an information security culture assessment in a financial organisation. The results of the analysis are used to identify areas for improving the information security culture assessment instrument. The study makes a contribution to the existing body of knowledge concerned with the assessment of information security culture and its value for management to ensure the protection of information assets.

Key words: information security, information security culture, information security awareness, behaviour, measure, assess, questionnaire, validity, reliability, survey

INTRODUCTION

Information security encompasses technology, processes and people (Von Solms 2000; Tessem & Skaraas 2005). It comprises a suitable set of controls such as organisational structures, software principles and e-mail practices implemented by the organisation. These information security controls are implemented to ensure the confidentiality,

Ms A. da Veiga and Prof. J.H.P. Eloff are in the Information and Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria. Prof. N. Martins is in the Department of Industrial Psychology, University of South Africa. E-mail: adele.daveiga@kpmg.co.za

integrity and availability of the organisation's information, which may be essential to maintaining a competitive edge, cash flow, profitability or legal compliance (ISO 2005).

Many organisations are at the stage where they have implemented technology and compiled information security policies and procedures to protect the organisation's information from a wide variety of threats. These threats could vary from computer-assisted fraud, espionage, sabotage and vandalism to fire. According to the Control Objectives for Information and related Technology (COBIT) Security Baseline Survival Kit (COBIT 2004), a lack of security awareness could cause a gap in an organisation's implementation of information security. Organisations now have to ensure that employees are aware of their responsibility in securing information assets such as archived information, system documentation, business strategies and databases (COBIT 2004; ISO 2005). Employees must also be adequately trained in order for the organisation to direct their behaviour to minimise accidental and malicious threats to information assets. The ISO17799 (ISO 2005) standard states that "providing appropriate training, education and awareness" is critical to the successful implementation of information security. It is therefore important that the members of an organisation's workforce are aware and conscious of information security in their daily work activities. In each organisation, an information security culture will emerge over time and become evident in the behaviour and activities of the workforce. This information security culture that develops can be defined as the assumption about those perceptions and attitudes that are accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organisation, with the aim of protecting information assets (Martins & Eloff 2002; Martins 2002). For organisations to manage security risks to information assets, they must have a strong information security culture (Baggett 2003; CITEC 2005; Dervin, Kruger & Steyn 2006; Gaunt 2000; ISF 2000; Martins & Eloff 2002; Ruighaver & Maynard 2006; OECD 2005; Stewart 2006; Schlienger & Teufel 2005; Tessem & Skaraas 2005; Thomson 2004; Von Solms 2006; Zakaria 2006).

Various factors motivate the importance of inculcating an information security culture in order to protect the information assets of organisations. The people who are expected to be responsible for information security constitute one of the main factors in this equation. Research illustrates that the interaction of people and the behaviour of employees towards computer and information assets represent the weakest link in information security (Abu-Musa 2003; Baggett 2003; Bresz 2004; Martins & Eloff 2002; Schlienger & Teufel 2002).

Based on a survey conducted by PricewaterhouseCoopers in 2004 (PWC 2004), a comparison was made between various surveys to illustrate the number of organisations that had experienced a security incident. As many as 83% of respondents indicated that they had experienced high-technology information security incidents. The three most common breaches were virus infections, staff

misuse of the Internet and physical theft of computer equipment. Although the number of technology incidents was very high, the report stated that "human error rather than technology is the root cause of most security breaches" (PWC 2004). According to PricewaterhouseCoopers, the solution would be to create a security-aware culture. Staff should be made more aware of the risks and of their responsibilities, thereby enabling them to act in a sensible and secure manner. The Guidelines for Security of Information Systems and Networks (Baggett 2003; OECD 2005) of the Organisation for Economic Cooperation and Development (OECD) provide a comprehensive framework for creating a culture of security. Through principles such as awareness, responsibility and ethics, a security culture will begin to develop – thereby minimising the threat that users pose to computer assets.

The organisation thus needs to ensure that an information security culture is inculcated through training, education and awareness in order to minimise risks to information assets. To determine whether the information security culture is at an acceptable level, it needs to be measured and reported on. One way of measuring the level of an organisation's information security culture is to use an information security culture assessment instrument (questionnaire) (Martins & Eloff 2002; Martins 2002; Schlienger & Teufel 2005). The results obtained from such an assessment can be used to identify areas for improving the protection of information assets.

AIM OF THIS PAPER

The aim of this paper is to validate an assessment instrument for assessing information security culture and provide one that is accepted as a valid and reliable assessment instrument in the information security and psychology research fields. In order to achieve the aim of the paper, an information security culture assessment was conducted in a financial organisation using an information security culture questionnaire.

CURRENT DEVELOPMENTS IN INFORMATION SECURITY CULTURE ASSESSMENTS

Perspective of the Information Security Forum

During November 2000, the Information Security Forum (ISF 2000) released a report discussing the definition of information security culture and the factors on which to focus when measuring it. They started their research in the realisation that despite compelling evidence that well-directed action can reduce information risks, incidents continue to occur on a daily basis. They concluded that this was probably due to a lack of a strong information security culture for driving down risk.

Based on the research work that the ISF conducted, they propose to develop a questionnaire to measure information security culture (ISF 2000). The main objective of the questionnaire would be for an organisation to identify the effect of information security culture on the organisation's level of information risk and specific target areas for improvement. As part of the ISF's future work, they plan to pilot the questionnaire at member firms, standardise it, enable benchmarking between organisations, and develop an implementation guide for organisations to use the measurement tool (ISF 2000).

Perspective of Schlienger and Teufel

Schlienger & Teufel (2002) introduced a paradigm shift – from a technical approach, towards information security, to a socio-cultural approach. They concluded that one has to focus on the organisational culture in addressing the human element so as to minimise risks to information assets and concentrate on the information security culture of the organisation.

Schlienger & Teufel (2003; 2005) selected the survey method, using a questionnaire, to obtain an understanding of the official rules that are supposed to influence the security behaviour of employees. Schlienger & Teufel's (2005) questionnaire takes into account the three levels of organisational behaviour of Robbins (2001), as well as research work performed by Schein (1985). It measures 20 areas (for example, leadership, problem management, communication and attitude). They performed substantive research to develop a decision-support system for analysing the results automatically and enabling employees to complete the questionnaire online. This tool was implemented in a private bank, and the application illustrated its usefulness. The Working Group on Information Security Culture of the Information Security Society of Switzerland (FGSec) also participated through discussions to ensure the practicability of the process. Schlienger & Teufel further aim to focus on extending the tool to allow benchmarking (Schlienger & Teufel 2005).

Perspective of Martins and Eloff

Martins and Eloff (Martins 2002; Martins & Eloff 2002) designed an information security culture model based on the concepts of organisational behaviour (Robbins, Odendaal & Roodt 2003) and what constitutes information security. They identified information security controls at the individual, group and organisational levels of organisational behaviour that could influence information security culture (Martins 2002; Martins & Eloff 2002). This theoretical perspective provided the basis for the information security culture questionnaire and the items developed by the researchers to assess information security culture (Martins 2002; Martins & Eloff 2002). The

information security culture questionnaire, however, still needs to be statistically standardised through a large enough sample so as to provide data that can be used to conduct a factor and reliability analysis that will ensure its validity and reliability.

MEASURING INSTRUMENT

The purpose of this paper is to validate the assessment instrument developed by Martins & Eloff (2002) and Martins (2002). The information security culture questionnaire developed by Martins & Eloff was selected, as it is based on an information security culture model addressing content validity (Brewerton & Millward 2001); moreover, its usefulness and practicality had already been proven in a case study (Martins 2002, Martins & Eloff 2002). This questionnaire was developed for use in environments where awareness programmes had already been implemented, as well as those where such programmes had not previously been implemented. It could therefore be applied in financial organisations, even if they had not implemented any awareness programmes. In addition, the information security culture questionnaire includes knowledge questions that are analysed separately from the information security culture statements. These questions assess awareness of employees pertaining to information security requirements that management expects employees to know. The knowledge questions can be used to obtain information pertaining to current knowledge of employees that could result in specific behaviour. If an employee does not know what an information security incident is, one could argue that he/she will not effectively report such incidents. This contributes to the practicability of the questionnaire, as the financial organisation specifically required the knowledge questions to determine how much employees know about information security in order for management to determine what principles to include in the first awareness programme.

The financial organisation also required specific information in terms of ethical conduct, trust and change management. This information was necessary to aid management in tailoring their awareness programme to address any concerns in these areas. For instance, if management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behaviour regarding information security. The perceptions of employees and management with respect to mutual trust need to be positive and should be regarded as a characteristic of the organisation that will aid in cultivating an information security culture from within. The information security culture questionnaire of Martins & Eloff focuses on these aspects and was found to be applicable to the requirements of the financial organisation. Apart from the data required by the researchers for the factor and reliability analysis, the financial organisation required the results of the survey for input to its awareness programme.

The information security culture questionnaire is divided into the following three sections (Martins 2002): (1) information security culture statements, (2) knowledge questions and (3) biographical questions.

Information security culture statements

This section assesses the perceptions of employees about eight different dimensions of information security: policies, management, programme, leadership, asset management, user management, change management and trust. A Likert scale (strongly agree, agree, unsure, disagree and strongly disagree) is used to answer the statements.

The following list reflects the statements in the information security asset management dimension:

- The organisation protects its information assets adequately (for example, systems and information).
- It is important to understand the threats to the information assets (for example, systems and information) in my department.
- Threats to security of information assets (for example, information and systems) are controlled adequately in my department.
- Information security is necessary in my department.
- The information assets (for example, systems and information) I work with need to be secured, either physically or electronically.
- I believe my business unit will survive if there is a disaster resulting in the loss of systems, people and/or premises.
- I feel safe in the environment I work in.
- I believe that the information I work with is adequately protected.

Knowledge questions

A section of knowledge questions is included to determine how much knowledge employees have about information security, and whether a low information security culture results from an educational problem or from perceptual concerns. A 'Yes/No' scale is used to answer these questions. The following five examples of knowledge questions are included in the information security culture questionnaire:

- The organisation has a written information security policy.
- I have read the information security policy sections that are applicable to my job.
- I know where to get a copy of the information security policy.
- I know what information security is.
- I know what an information security incident is.

Biographical questions

Biographical questions are included in the information security culture questionnaire in order to segment the data and draw comparisons within the population, for instance with regard to job levels or departments, as indicated by the following question:

What is your job level?

- Executive and senior managers
- Department managers and supervisors
- Operational staff (administrative, clerical, sales, etc.)
- Technology staff.

SURVEY METHODOLOGY

The survey methodology serves as a method that organisations can use to study information security behavioural content in general, as well as the attitude and opinions (Berry & Houston 1993) of employees with respect to information security in particular. This method is used to systematically gather data from members of an organisation for a specific purpose (Kraut 1996).

The process of designing, implementing, administering and reporting back on survey data is key to the success of the survey and perhaps even more important than the actual results generated (Kraut 1996). According to Berry & Houston (1993) and Kraut (1996), the main phases of a survey methodology should include planning and preparation, survey administration, data analysis, report writing and feedback to management and employees. Planning and preparation involve the participation of stakeholders, the customisation of the questionnaire, decisions on the population and sample size and a pilot study (Berry & Houston 1993; Church & Waclawski 1998). During the administration of the survey, the survey is communicated to the population and responses are monitored. The data are then statistically analysed, whereafter the report is compiled and feedback sessions are held to discuss action plans (Church & Waclawski 1998).

The following section discusses the survey methodology by illustrating how it was implemented in the financial organisation in order to obtain the data required for the factor and reliability analysis.

Planning and preparation

The first step in conducting a survey is to plan it (Berry & Houston 1993). The information security culture survey in the financial organisation was initiated through a formal project introduction meeting to obtain buy-in from relevant stakeholders and to discuss the project plan of operations (Berry & Houston 1993). As part of this meeting, the concept of information security culture was discussed, as well as the

approach that would be followed in conducting the survey. The stakeholders involved consisted of representatives from various departments – IT, information security, governance, risk management, human resources and training. The project sponsor was the Information Security Officer (ISO), and the various stakeholders assisted with the survey communication, technology set-up and coordination of the project across the target population to ensure that the required responses were obtained.

The second step was to conduct a workshop with the organisation's project team so as to customise the questionnaire (Berry & Houston 1993) developed by Martins (2002). IT as well as business representatives participated. Organisation-specific terminology was added to the information security culture questionnaire statements. The knowledge section of the information security culture questionnaire was also adjusted to incorporate questions specific to the environment of the organisation and any security awareness initiatives undertaken in the past. For instance, since the organisation has not rolled out an information security awareness programme in the past, no questions pertaining to such a programme were asked. The biographical questions were finalised based on the selected target population. These questions covered the business areas, geographical areas, length of service and job levels with respect to the organisation. It was decided that the information security culture questionnaire would be sent out to all employees in the selected business areas, altogether 12 572 employees. This method is referred to as convenience sampling (Brewton & Millward 2001).

Before the information security culture questionnaire could be rolled out to the target population, it had to be pretested on a small sample of employees to allow the researcher to understand the anticipated reactions of the larger group and to revise or restructure questions where necessary (Berry & Houston 1993). A group of 20 employees in the organisation completed the pilot survey in order to test the face validity of the information security culture questionnaire. Face validity is concerned with whether the questionnaire assesses what it says it does on the 'face of it' (Furnham & Gunter 1993). Minor adjustments were made to some of the culture statements to ensure that all employees would interpret the statements in the same manner. For instance, examples were added to some terms, and the word 'department' was changed to 'business area' as indicated in the box.

> My *business area* protects its information assets adequately *(e.g. systems and information in electronic or paper format)*.

The survey tool, Survey Tracker (2005), was used as the survey software to distribute, capture and conduct the survey analysis (Berry & Houston 1993). The information security culture questionnaire that was signed-off by the ISO had been designed in HTML format in Survey Tracker according to the scientific rules of

scales and question types built into the software. In collaboration with the IT department, a link to the information security culture questionnaire was added to the organisation's Intranet site, where employees could complete it. Figure 1 is an example of two statements extracted from the HTML-designed information security culture questionnaire.

	Strongly disagree	Disagree	Uncertain	Agree	Strongly agree
14. Information security should be part of key performance measures for the employees of the Group	•	•	•	•	•
15. Employees should be monitored on their compliance to information security policies and procedures (e.g. measuring the use of e-mail, monitoring which sites an individual visits or what software is installed on personal computes).	•	•	•	•	•

Figure 1: Extract from information security culture questionnaire

Survey administration

Communicating the survey and its objectives to employees is crucial in order to enhance the response rate and the quality thereof (Dillon, Madden & Firtle 1993). If questions are of a sensitive nature, and employees wish to remain anonymous, the organisation must ensure that individual responses cannot be identified (Berry & Houston 1993). For the purpose of this survey, the responses of the completed information security culture questionnaires were automatically saved in a file on one of the organisation's secure servers.

A communication e-mail was sent out to all employees from the 'Communication' mailbox a week before the survey was launched to prepare them for and inform them of the forthcoming survey. The survey ran for four weeks, during which employees were continually encouraged to complete the information security culture questionnaire online.

During this period, the responses were tracked to ensure that a statistically representative response was obtained for each biographical area into which the data would be segmented. Table 1 provides a summary of the divisions of the organisation, the number of employees in each, the statistically representative sample required and the actual response obtained. The method designed by Krejcie & Daryle (1970) was used to determine the required sample size. In only four divisions was this not representative. Trends were considered for these divisions.

When a validity test is conducted, the commonly accepted criterion is to have at least 100 respondents, or five times the number of responses compared to the number

of questions in the questionnaire (Martins 2000). The more accepted criterion is to have at least ten times the number of responses. This will ensure that the conclusions drawn from the sample data are not sample specific and that it is possible to generalise the findings (Martins 2000). The information security culture questionnaire consists of 42 statements that were used in the factor and reliability analysis. Overall, a representative number of 4 735 employees participated in the survey, which was a more than adequate sample.

Table 1: Information security culture questionnaire – representative sample

Division/ Business unit	Total number of employees	Sample required based on Krejcie & Daryle method	Actual responses	Representative (Yes/No)
Division A	1 847	318	1 213	Yes
Division B	261	155	160	Yes
Division C	1 146	217	500	Yes
Division D	132	75	93	Yes
Division E	3 481	346	675	Yes
Division F	668	191	381	Yes
Division G	1 311	224	536	Yes
Division H	311	172	124	No
Division I	660	245	209	No
Division J	72	61	42	No
Division K	77	64	40	No
Division L	2 606	335	545	Yes
Division M	No data	No data	144	No data
No response	n/a	n/a	73	n/a
Overall	12 572	355	4 735	Yes

Statistical analysis and results of the survey

The survey results were analysed using Survey Tracker (2005). Figure 2 shows the job levels of respondents. The respondents represented all job levels in the organisation: executive and senior managers (3.97%), department managers and supervisors (21.94%), operational job staff (64.16%) and technology staff (8.51%). Most respondents had worked for the organisation for more than ten years (32.06%) or for between 5 and ten years (23.59%), 77.4% worked at head office, and the rest at

branch offices. Responses were received from all nine provinces in South Africa, with the majority from Gauteng (62.09%), followed by the Western Cape (12.61%) and KwaZulu Natal (9.17%).

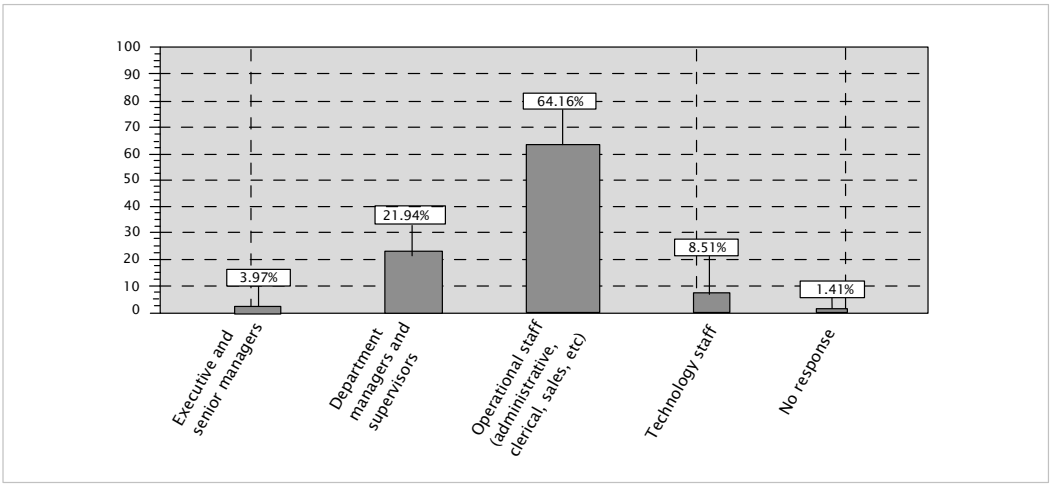

Figure 2: Job levels of respondents

Figure 3 shows the results of three of the knowledge questions as an example. The first column lists the question, the second provides the number of people that responded to the question, and the last column gives the percentage of people that answered 'Yes'. The figure illustrates that only 70.2% of the 4 691 respondents that answered the last question know where to get a copy of the information security policy. This would indicate that the organisation needs to communicate to employees where to obtain a copy of the information security policy and to ensure that the policy is kept or saved in a location where it is easy for employees to access it.

Statements	Count	Percentages of 'Yes' responses 0 20 40 60 80 100
The organisation has a written information security policy.	4 584	94.9%
I know what information security is.	4 690	92.2%
I know where to get a copy of the information security policy.	4 691	70.2%

Figure 3: Knowledge statement results

This concludes the discussion pertaining to the survey methodology used to conduct the information security culture assessment in the financial organisation in order to obtain data that could be used to validate the information security culture questionnaire.

FACTOR AND RELIABILITY ANALYSIS

The concept of validity implies that the researcher must ensure that the questionnaire assesses what it claims to assess (Berry & Houston 1993; Dillon, Madden & Firtle 1993; Furnham & Gunter 1993). Over time, such a questionnaire will yield reliable and stable results that prove to be valid (Dillon, Madden & Firtle 1993). Construct validity is considered for the validity analysis of the information security culture questionnaire. Construct validity is established using the principle components factor analysis to assess the robustness of the questionnaire dimensions, thereby identifying clusters of questions (statements) and forming new dimensions (Brewerton & Millward 2001). In the industrial psychology literature and in research, factor analysis is frequently used to assess whether instruments (questionnaires) measure substantive constructs which in this case are the nine dimensions of the information security culture questionnaire. Factor analysis as a statistical technique is employed to determine or uncover any underlying 'structure' that may exist in a data set (Brewton & Millward 2001; Howell 1995). It has various applications, which include establishing the structure of 'traits' that underlie personality, understanding the relationship between various performance criteria, and exploring the relationship between established work-related constructs (for example, leadership, communication, governance, awareness) (Brewton & Millward 2001; Martins & Von der Ohe 2003).

The principal components factor analysis (PCA) is a data analysis tool that is generally used to reduce the dimensionality (number of questions or statements) of a large number of interrelated questions, while retaining as much of the information (variation) as possible (Hintze 1997). The Number Cruncher Statistical Software (NCSS) program (Hintze 1997) was used for this purpose.

The latent root criterion (Hair, Anderson, Tatham & Black 1995), which specifies that all factors with eigenvalues of 1.00 or greater should be retained, was used. The eigenvalues are helpful in determining the variance of each factor and thus how many factors should be retained. The use of the eigenvalue as a cut-off point is possibly the most reliable criterion in determining how many factors to retain. All factors with a factor value greater than 1.00 were retained (Hintze 1997).

An initial factor extraction was done according to PCA, and the inter-correlation matrix was rotated according to the varimax method using the NCSS tool. The varimax method is used to obtain new factors or dimensions that are each highly correlated with only a few of the original variables (Hintze 1997).

Next, the reliability of each factor was determined by means of an item analysis (Cronbach alpha) that examines the correlation between each item and the scale total within a sample (Brewerton & Millward 2001). An item analysis is used to examine the frequencies and descriptive statistics for each item on the survey across all responses obtained (Church & Waclawski 1998). Reliability testing (Brewerton &

Millward 2001) is concerned with the degree of data consistency across a defined dimension. The purpose of both these techniques is to determine the reliability of an instrument (questionnaire). Both techniques were employed to assess whether the security culture instrument measures the substantive constructs (dimensions) and to test the reliability thereof.

DISCUSSION

The variance rotation isolated four factors, as listed in Table 2, which could be used as the four new information security culture dimensions and which accounted for 53.3% of the variance. According to Hintze (1997), factors that account for at least 50% of the variance are accepted. The interpretation of the factor matrix showed that none of the statements had a factor loading lower than 0.30, which is regarded as the cut-off point. According to Hair et al. (1995) a factor loading above 0.30 is regarded as meaningful and can be included in the dimensions. The internal consistency of the four new dimensions varies between 0.955795 and 0.676533 (Table 3). According to Brewton & Millward (2001), internal reliabilities between 0.6 and 0.7 are generally accepted as an absolute minimum to be identified as a factor.

Table 2: Results of initial factor analysis

Factor	Statement numbers
Factor 1	14, 15, 16, 22, 25*, 26, 28, 30, 33, 35, 38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 51, 52, 53
Factor 2	12, 17, 21, 23, 24, 25, 27, 28, 29, 31, 34, 36, 37
Factor 3	13, 18, 19, 22
Factor 4	45, 49, 50

* Item 25 loads high on factors 1 and 2

Table 3: Reliability analyses of initial analysis

Factors	Cronbach alpha	Number of items/ statements	Comments
Factor 1	0.955795	24	Item 25 loads high on factors 1 and 2
Factor 2: Management of information security	0.890352	16	
Factor 3: Performance management	0.677747	4	Item 22 loads high on factors 1 and 3
Factor 4: Performance accountability	0.676533	3	

A second-phase factor analysis was conducted for factor 1 in order to determine whether sub-dimensions could be formed. The same techniques and criteria were used as with the first analysis. The factors and factor loadings are presented in Tables 4 and 5. The factor loadings range between 0.807570 and 0.933200.

Table 4: Results of the factor analysis for the second-phase analysis – Factor 1

Factor	Statement numbers
Factor 5: Communication	22, 33, 35
Factor 6: Governance	14, 15, 16, 20, 25, 26, 30
Factor 7: Capability development	38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 51, 52, 53

Table 5: Reliability analysis of second-phase analysis

Factors	Cronbach Alpha	Number of items
Factor 5: Communication	0.807570	3
Factor 6: Governance	0.891884	7
Factor 7: Capability development	0.933200	14

Naming of factors

Conceptual naming of factors 2 to 7 was done after detailed inspection of the individual items (statements). The purpose was to attach a dimension name to each factor to make it understandable and identifiable for the information security culture questionnaire. Each of the new information security culture dimensions will next be discussed briefly.

Management of information security (factor 2)

This dimension includes the applicability of the information security policy, the understanding of threats to information assets, a willingness to change working practices to ensure the security of information assets and an acceptance of a responsibility towards information security.

Performance management (factor 3)

The items included in this dimension determine whether information security should be part of key performance measures, whether employees believe that they should be monitored, and whether the contents of the information security policy had been effectively explained to them, thus enabling employees to adhere to the policy.

Performance accountability (factor 4)

This dimension focuses on aspects such as whether action should be taken against people that do not adhere to the information security policy, whether employees feel safe where they work and whether people should be held accountable for their actions if they do not adhere to the information security policy.

Communication (factor 5)

The items included in this dimension focus on aspects such as the explanation of the information security policy, informing employees in a timely manner how information security changes will affect them, and informing people about what is expected of them regarding information security.

Governance (factor 6)

This factor focuses on aspects such as whether management adheres to the information security policy, the adequate protection of information assets, the perception of the importance of information security, and adequate control over information security assets.

Capability development (factor 7)

This dimension focuses on a number of aspects relating to employee trust, the commitment of time to information security, adherence to the information security policy by the various business areas, commitment to the policy and a belief that information is adequately protected.

This questionnaire with the six revised dimensions is hereafter referred to as the Information Security Culture Assessment (ISCA) questionnaire. Table 6 details the eight dimensions of the original information security culture questionnaire compared with the six new dimensions of the ISCA, as well as the number of statements per dimension. The six new dimensions have been constructed on the basis of the factor and reliability analysis as discussed, thereby ensuring that the new information security culture questionnaire meets the requirements for a reliable questionnaire as accepted in the statistical field.

After an analysis had been conducted of each of the items (statements) in the six ISCA dimensions, the items were regrouped and applicable names were given to each group of items relating to a single concept. The individual statements were left unchanged. Figure 4 illustrates the composition of the dimensions and groups the items into the identified concepts that are measured in each dimension.

For example, the management of the information security dimension involves four main concepts that are measured, namely accepting ownership, accepting change,

Table 6: Comparing the old and revised information security culture dimensions

Old information security culture questionnaire dimensions (factors)	Number of statements per dimension (factors)	New information security culture dimensions (factors) of ISCA	Number of statements per dimension (factors)
Information security policies	2	Management of information security	12
Information security management	2	Performance management	4
Information security programme	7	Performance accountability	3
Information security leadership	8	Communication	3
Information asset management	8	Governance	7
User management	8	Capability development	14
Change management	4		
Trust	3		
Total number of items	**42**	**Total number of items**	**43**

necessity of resources and understanding threats. The items (statements) in the information security culture questionnaire will determine users' perceptions with regard to each of the four concepts.

Table 7 outlines the statements of the revised governance dimension (previously the information assets management dimension) in order to illustrate how the statements were regrouped on the basis of the factor analysis.

CONCLUSION AND RECOMMENDATIONS

The paper addressed its purpose by validating an information security culture questionnaire. This was enabled by conducting an information security culture assessment in a financial organisation and using the data to perform a factor and reliability analysis. As output, a revised information security culture questionnaire is proposed that yields reliable results should it be used to assess information security in other organisations or as a follow-up assessment in the financial institution to benchmark the results.

In the light of the research results, it is evident that there are revised or possible additional dimensions that could be constructed for the information security culture questionnaire. Based on the assessment that was conducted, as well as other organi-

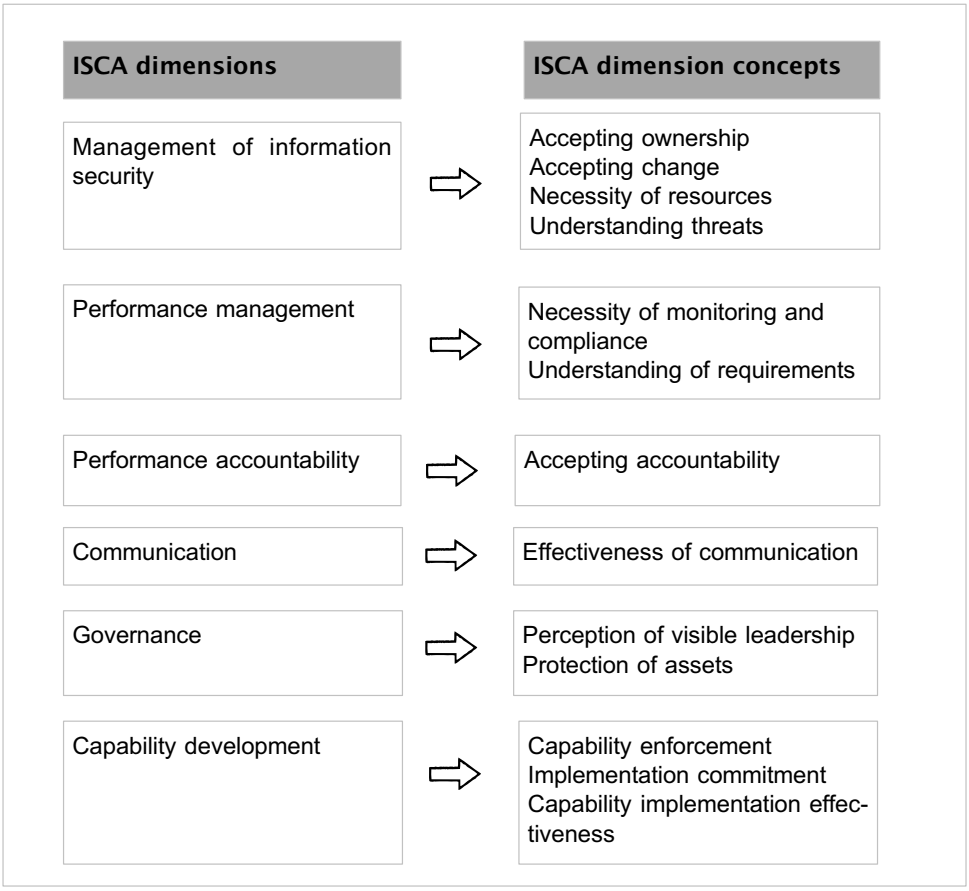

Figure 4: ISCA dimensions and concepts

Table 7: Governance dimension statements

Governance concepts	**Governance dimension statements (items)**
Perception of visible leadership	1 Management in my department **adheres** to the information security policy.
	2 Department managers and supervisors perceive information security as **important**.
	3 Executive and senior management perceive information as **important**.
	4 Information security is perceived as **important in** my business area.
	5 The staff in our department perceive information security (e.g. sharing confidential information) as **important**.
Protection of assets	6 My business area **protects** its information assets adequately.
	7 Threats to security of information assets are **adequately controlled** in my department.

sations where the information security culture assessment was conducted, it was determined that certain aspects of the information security culture questionnaire could be further enhanced to meet the needs of the industry. The following should be considered when further enhancing ISCA:

- The dimension on user knowledge and awareness could be enhanced to enable more in-depth correlations to the culture statements.
- Attention should be focused on ethical considerations and the perception of users with regard to sensitive information.
- More attention should be focused on communication in terms of what the preferred channels are and how effective employees perceive them to be.
- The performance measurement, performance accountability and communication dimensions of ISCA could be expanded to include at least three to five statements per dimension (Church & Waclawski 1998).
- The completeness of the regrouped statements in the new dimensions should be investigated. For example, the governance dimension should be assessed to identify all concepts of governance that pertain to an information security culture in order to ensure the completeness of the statements in each ISCA dimension.

REFERENCES

Abu-Musa, A.A. 2003. 'The perceived threats to the security of computerized accounting information systems', *Journal of American Academy of Business,* 3(1/2): 9–20.

Baggett, W.O. 2003. 'Creating a culture of security', *Internal Auditor*, 60(3): 37–41.

Berry, M.L. & Houston, J.P. 1993. *Psychology at Work*. Winsconsin: Brown and Benchmark.

Bresz, F.P. 2004. 'People – Often the weakest link in security, but one of the best places to start', *Journal of Health Care Compliance*, 6(4): 57–60.

Brewton, P. & Millward, L. 2001. *Organizational Research Methods*. London: Sage.

Church, A.H. & Waclawski, J. 1998. *Organizational Surveys – a Seven Step Approach*. San Francisco, CA: Jossey-Bass.

CITEC. 2005. 'Building a strong security culture'. [Online] Available at: www.citec.com.au/news/featureNews/2005/April/security_culture.shtml. Accessed: January 2006.

COBIT (Control Objectives for Information and related Technology). 2004. *COBIT Security Baseline – An Information Security Survival Kit*. USA: IT Governance Institute.

Dervin, L., Kruger, H. & Steyn, T. 2006. 'Value-focused assessment of information communication and technology security awareness in an academic enviornment', *Security and Privacy in Dynamic Environments*, pp 448–453. IFIP International Federation for Information Processing, 201.

Dillon, W.R., Madden, T.J. & Firtle, N.H. 1993. *Essentials of Marketing Research*. Boston: Irwin.

Furnham, A. & Gunter, B. 1993. *Corporate Assessment: Auditing a Company's Personality.* London: Routledge.

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

Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. 1995. *Multivariate Data Analysis with Readings*, 4th edition. Englewood Cliffs, NJ: Prentice Hall.

Hintze, J.L. 1997. *Number Cruncher Statistical Systems,* version 5.03 5/90. Kaysville, UT: NCSS.

Howell, D.C. 1995. *Fundamental Statistics for the Behavioral Sciences,* 3rd edition. International Standards Organisation. [Online] Available at: www.iso.ch. Accessed: January 2005.

ISF (Information Security Forum). 2000. *Information Security Culture – A Preliminary Investigation*. United Kingdom: ISF.

ISO. 2005. Information technology. Security techniques. Code of practice for information security management. ISO/IEC 17799 (BS 7799–1: 2005).

Kraut, A.I. 1996. *Organizational Surveys*. San Francisco, CA: Jossey-Bass.

Krejcie, R.V. & Daryle, M.W. 1970. 'Determining sample size for research activities', *Educational and Psychological Measurement*, 30.

Martins, A. 2002. 'Information security culture', MCom dissertation, Rand Afrikaans University, Johannesburg.

Martins, E.C. 2000. 'Die invloed van organisasiekultuur op kreatiwiteit en innovasie in 'n universiteitbiblioteek', MCom dissertation, University of South Africa, Pretoria.

Martins, A. & Eloff, J.H.P. 2002. 'Information security culture', *Security in the Information Society,* pp. 203–214. IFIP/SEC2002. Boston, MA: Kluwer Academic Publishers.

Martins, N. & Von der Ohe, H. 2003. 'Organisational climate measurement – new and emerging dimensions during a period of transformation', *South African Journal of Labour Relations,* (27)3 & 4: 41–59.

PWC (PricewaterhouseCoopers). 2004. Information Security Breaches Survey. [Online] Available at: www.dti.gov.uk/industry_files/pdf/isbs_2004v3.pdf. Accessed: January 2005.

Robbins, S. 2001. *Organizational Behaviour,* 9th edition. New Jersey: Prentice Hall.

Robbins, S., Odendaal, A. & Roodt, G. 2003. *Organisational Behaviour – Global and Southern African Perspectives*. Cape Town: Pearson Education.

Ruighaver, A.B. & Maynard, S.B. 2006. 'Organisational security culture: More than just an end user phenomenon', *Security and Privacy in Dynamic Environments*, pp 425–430, IFIP International Federation for Information Processing, 201.

Schein, E.H. 1985. *Organizational Culture and Leadership*. San Francisco, CA: Jossey-Bass.

Schlienger, T. & Teufel, S. 2002. 'Information security culture', *Security in the Information Society*, pp 191–201. IFIP/SEC2002. Boston, MA: Kluwer Academic.

Schlienger, T. & Teufel, S. 2003. 'Analysing information security culture: Increased trust by an appropriate information security culture', Paper presented at International Workshop on Trust and Privacy in Digital Business Trust in conjunction with 14th International Conference on Database and Expert Systems Applications, Prague, Czech Republic.

Schlienger, T. & Teufel, S. 2005. 'Tool supported management of information security culture', Paper presented at 20th IFIP International Information Security Conference, Makuhari-Messe, Chiba, Japan.

Stewart, J.N. 2006. 'CSO to CSO: Establishing the security culture begins at the top'. [Online] Availabe at: cisco.com/web/about/security/intelligence/05_07_securityculture.html. Accessed: January 2006.

Survey Tracker. 2005. [Online] Available at: www.surveytracker.com. Accesed: January 2005.

Tessem, M.H. & Skaraas, K.R. 2005. 'Creating a security culture'. [Online] Availabe at: www.telenor.com/telektronikk/volumes/pdf/1.2005/Page_015–022.pdf. Accessed: January 2006.

OECD (Organisation for Economic Cooperation and Development). 2005. 'The promotion of a culture of security for information systems and networks in OECD countries (OECD)', DSTI/ICCP/REG(2005)1/FINAL.2005. [Online] Available at: www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html. Accessed: August 2006.

Thomson, I. 2004. 'IT security culture must start from the top Global survey warns senior execs against "delegating" security awareness'. [Online] Availalbe at: www.vnunet.com/vnunet/news/2125904/securityculturestarttop. Accessed: January 2006.

Von Solms, B. 2000. 'Information security – the third wave?' *Computers and Security*, 19(7): 615–620.

Von Solms, B. 2006. 'Information security – the fourth wave', *Computers and Security,* 25 (2006): 165–168.

Zakaria, O. 2006. 'Internalisation of information security culture amongst employees through basis security knowledge', *Security and Privacy in Dynamic Environments*, pp 437–441. IFIP International Federation for Information Processing, 201.