Assessing Information Security Culture

A. MARTINS1, JHP ELOFF[2]

[1] adele.martins@kpmg.co.za
Rand Afrikaans University, Johannesburg, South Africa
[2] eloff@rkw.rau.ac.za
Department of Computer Science
Rand Afrikaans University
PO Box 524
AUCKLAND PARK
2006
South Africa
2001
Tel: +27 11 489-2847   Fax: +27 11 489

Key words: information security culture, assessment, audit, behaviour

Abstract: The behaviour of employees and their interaction with computer systems have a significant impact on the security of information. Human interaction with information resources is often the weakest link in protecting Information assets. One way of addressing it is by focusing on positively changing the culture of the organisation. In order to do this a model is proposed which can be implemented by an organisation. An assessment approach consisting of an audit process and incorporating an information security culture questionnaire is discussed as the main focus of this paper.

1. INTRODUCTION

People are the center of every activity. They invented information technology (IT), they drive it, develop it, but also pose the most serious threat, whether intentional or unintentional, to information used in the IT environment. Protecting information used in the wider business context should therefore also incorporate the behaviour of people. People manage the information in an organisation and interact with IT systems.

Each organisation has its own information security culture similarly to every person having its own personality. A positive information security culture can aid in minimising the people threat compromising information security while interacting with IT systems.

This paper discusses what an information security culture is and proposes a model to positively enhance the information security culture of an organisation. The focus is on the development of an information security culture questionnaire and audit process to promote information security culture in an organisation.

2. INFORMATION SECURITY CULTURE

The behaviour of employees towards information must be acceptable and needs to be part of everyday life in the organisation. An example of such behaviour could be the confidential handling of client information or that only authorised maintenance personnel may service computer equipment.

Every organisation also has certain information security practices, which are followed and incorporated into the working environment. This will become part of the organisational culture. An example of such a practice is to change passwords every week or to get an auditor to assess the organisation's computer networks.

To facilitate the above, it is necessary to cultivate an information security culture in the organisation [VONS00, ELOFF00, MCLU00]. Information security culture can be seen as the following:

- **Information security culture is a set of information security characteristics that the organisation values**

These characteristics, such as integrity, confidentiality and availability of information, need to be valued and pursued by the organisation. For instance, for a health care organisation, privacy issues will be a much more important characteristic to pursue in order to protect patient records compared to the customer records of a retail store.

- **Information security culture is the assumption about what is acceptable and what is not in relation to information security**

It may not, for instance, be acceptable to discard of a confidential document by depositing it in a garbage can, but to rather shred it. Another example is that it is not acceptable to leave crucial business information in office areas where anyone could access or read it; it should rather be locked away. By instilling an information security culture, information security practices such as a clear desk policy and controls such as encryption will be accepted as the way things are done.

- **Information security culture is the assumption about what information security behaviour is encouraged and what is not**

Information security culture will also emerge from encouraging acceptable information security behaviour. An example could be that people are encouraged to report security incidents via the appropriate management channels. Management could also encourage employees to regard the work they do as part of the organisation's intellectual property, which needs to be protected.

- **Information security culture is the way people behave towards information security in the organisation**

People have their own attitudes towards different situations and processes in an organisation. These attitudes could be positive or negative and have an impact on the way people behave. Their attitude towards information security and how they perceive it will result in certain behaviour. If they do not accept a clear desk policy and feel negative about it, they will not take care in putting confidential documents away and so not behave according to what is expected of them.

3. INFORMATION SECURITY CULTURE MODEL

Organisational behaviour plays an important role in the development of an organisational culture. Through the culture it will be clear what behaviour is accepted and encouraged and what is not. This can then be traced back to management's vision and strategies.

To establish the desired culture in an organisation, it is necessary to take a look at the organisational behaviour of the employees. The type of culture in an organisation can have a direct impact on the behaviour and actions of the organisation's employees [MART00]. In an organisation with a bureaucratic culture, where everyone has to play by the rules, employees might follow the information security policy more strictly than in a less formal and individualistic culture [YEAT96].

Changing an organisation's culture will in effect then also require the focus to be on changing ineffective behaviour and procedures and not the organisational culture [HELL98].

In order to incorporate organisational behaviour to instil an information security culture the organisational behaviour model of Robbins was used to construct an information security culture model depicted in figure 1. This model consists of three basic levels namely, the organisational, group and individual level. Issues that could promote the information security culture were identified on each of these to levels. These issues will be affected through change agents and will as output result into a certain information security culture.

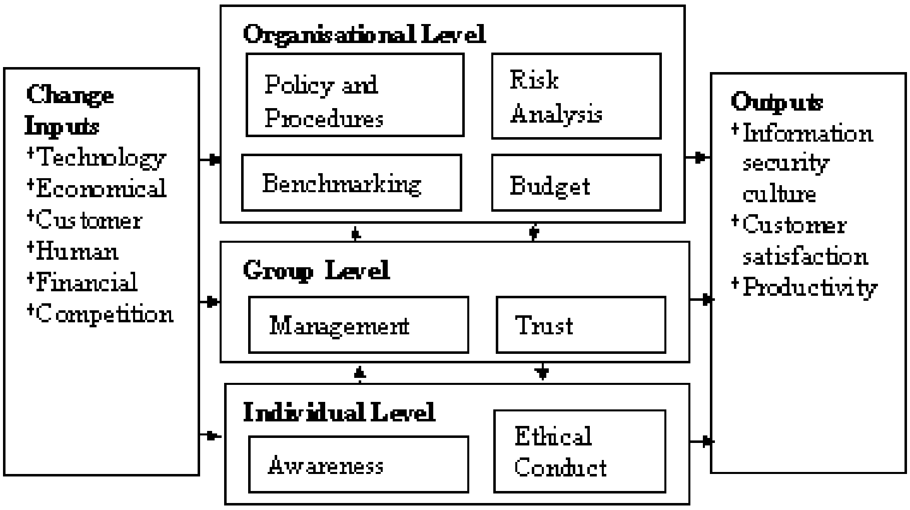


Figure 1. Information Security Culture Model

4. INFORMATION SECURITY CULTURE ASSESSMENT APPROACH

An assessment approach was developed to aid an organisation to determine whether they have an adequate level of information security culture in the organisation.

The assessment approach consists of an audit process where the perceptions, attitudes, opinions and actions of employees regarding information security can be determined. By analysing this information, an organisation can assess how employees perceive information security activities and which aspects concerning information security culture at the three levels need attention.

The information security culture audit process consists of four phases:

- In phase 1, the assessment instrument, namely the information security culture questionnaire, is developed. The information security culture model's issues are used to identify and develop questions or statements for the questionnaire. A questionnaire framework is put together which can be customised for different organisations' specific needs.

- Phase 2 consists of the survey process where the actual assessment takes place by using the information security culture questionnaire as developed in phase 1. Phase 2 can be used by organisations to assess their information security culture environment. It is seen as a continuous process to promote the information security culture of an organisation. By conducting for instance yearly assessments and implementing and addressing the interpretations and recommendations of a previous assessment the organisation can continuously improve its information security culture.

- In phase 3 the data, obtained as the output of phase 2, is analysed. These results give a quantitative indication of the status of the information security culture. This data gives the organisation a high level picture of the level of information security culture as well as specific information about positive and developmental areas.

- Phase 4 addresses the interpretations and recommendations regarding the analysed data that was obtained in phase 3. This enables the auditor to provide the organisation with feedback of the information security culture environment in the organisation with the goal of promoting the culture by addressing the developmental areas. In order to facilitate this it might for instance be necessary to roll out an awareness campaign or to improve information security policies.

A case study was conducted to develop the information security culture questionnaire framework. This framework was found to be adequate to assess an organisation’s information security culture. The case study was also used to illustrate the information security culture audit process an organisation can follow. The four audit phases will now be discussed with reference to the case study.

4.1 Phase one: Develop questionnaire

The information security culture questionnaire’s main purpose is to assess the information security culture of an organisation by focusing on the behaviour and perceptions of employees regarding the three levels of the information security culture model.

Key issues (dimensions) were identified from the information security culture model and statements or questions for each sub-dimension were constructed. Before the actual questions were developed, certain criteria were considered. For instance, questions need to be brief and clear to ensure understandability for the respondents. The language ability of the respondents should also be considered by constructing statements or questions without jargon and unknown abbreviations. It is also critical to construct a statement with only one concept, issue or problem to ensure that the data will be analysed and interpreted correctly [BERR93, DILL93, PORT, WALT96].

For the purpose of the information security culture questionnaire, which aims to assess perceptions and attitudes, a Likert scale was used. Likert scales are very popular with researchers because of their simplicity and power. They measure the respondent’s degree of agreement or disagreement with other respondents, thus providing the ability to derive an aggregate score when all the answers are combined [SURV00]

Two concepts were taken into account when developing the draft questionnaire, namely validity and reliability [FURN93]. The concept of ‘validity’ implies that the researcher must ensure that the questionnaire assesses what it claims to assess [BERR93, DILL93, FURN93]. The information security culture questionnaire focuses specifically on **face validity**. Face validity is concerned with whether the questionnaire looks as if it is assessing what it says it does on the “face of it” [FURN93].

The term 'reliability' refers to the consistency with which the measures of the assessments are reproduced. In other words, if the sample group completes the questionnaire repeatedly over a period, the results should be similar, taking into account that the variable measured remains the same [BERR93, DILL93, FURN93].

Pilot study

When an organisation wants to assess its information security culture it is important to get management and stakeholders involved from the beginning. They need to understand and accept that information security is a priority for the organisation and that they also play a role in establishing an acceptable information security culture.

An organisation needs to customise the information security culture questionnaire that was developed This can be done through involving key players like IT management, the chief information security officer, but also employees who are using IT facilities like clerks and secretaries through interviews and/or focus groups. They need to give their perception of what they think is necessary to assess regarding information security culture in the organisation. Their input should then be used to draft an information security culture questionnaire based on the framework questionnaire. A pilot study should also be conducted to ensure that all employees would be able to interpret questions in the same way and so ensure the validity of the questionnaire. The pilot test further determines the clarity of instructions, readability, relevance and user interactions.

4.2 Phase 2: Survey process

If an organisation wants to assess its information security culture, the entire population needs to be included in the audit process. The population can be seen as the entire workforce of the organisation, in other words all employees who are working in the organisation. This is necessary since the culture of one office to the next and one department to the next could be different. By getting all employees to participate, comparisons can be made between offices, departments and job levels. It is often unrealistic to involve all employees if the organisation has a large workforce. A sample that represents the workforce can then be used to participate in the audit.

To conduct the survey process the Internet, intranet or an e-mail approach is suggested since it makes the questionnaire collection and data capturing process easier and also saves time. In cases where technology cannot be used paper questionnaires can be used which needs to be captured into a database to analyse the data.

It is important that questionnaires are answered anonymously and send to an independent party. This will ensure confidentiality and employees will feel more confident to give their opinion if they know they cannot be identified.

4.3 Phase 3: Analyse data

Survey Tracker [SURV00], a statistical software program, was used to analyse the data of the information security culture questionnaire to ensure that the correct interpretations and correlations between different groups like management and employees or departments are made.

Figure 3 gives the frequency distribution of the four dimensions, namely the organisational, group, individual as well as change dimensions. The frequency distribution is the frequency with which a variable occurs, i.e. how often a specific score occurs [HOWE95].

Each bar represents the percentage of respondents who indicated that they felt positive or favorable about the statements portrayed in the dimension. A cut-off of 64% on the frequencies was used. This percentage provides a reasonable cut-off to distinguish between positive and potential negative perceptions [ODEN97].

Each of the four dimension’s results is independent from each other and indicates the perception of the population who participated in the audit. It does not for instance reflect the actual organisation structures or individual knowledge on information security, but the information security culture. In other words it portrays the way people perceive issues regarding information security.

It is evident from figure 2 that the organisational and change dimension falls below the 64% cut-off indicated by the red horisontal line. This indicates that these dimensions are critical developmental areas.

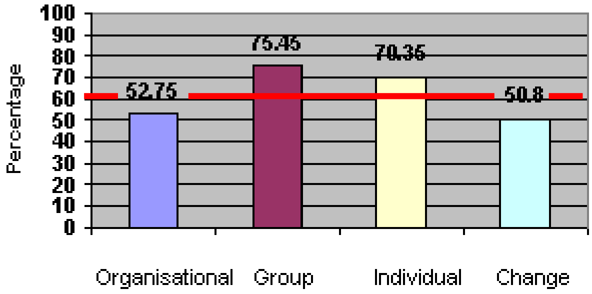


Figure 2. Dimensions

In order to interpret the results of the case study, it is necessary to study the results of each of the nine sub-dimensions in detail. From the results the auditor will be able to draw conclusions and interpret the findings in order to provide recommendations to the organisation.

Figure 3 indicates the frequency distribution of the nine sub-dimensions. Five of the nine sub-dimensions fall below the cut-off. The developmental sub-dimensions are policy and procedures, benchmarking, management, ethical conduct and change. Ethical conduct is, however, on the cut-off and can therefore be seen as an area that is not as critical to develop as the other four sub-dimensions.

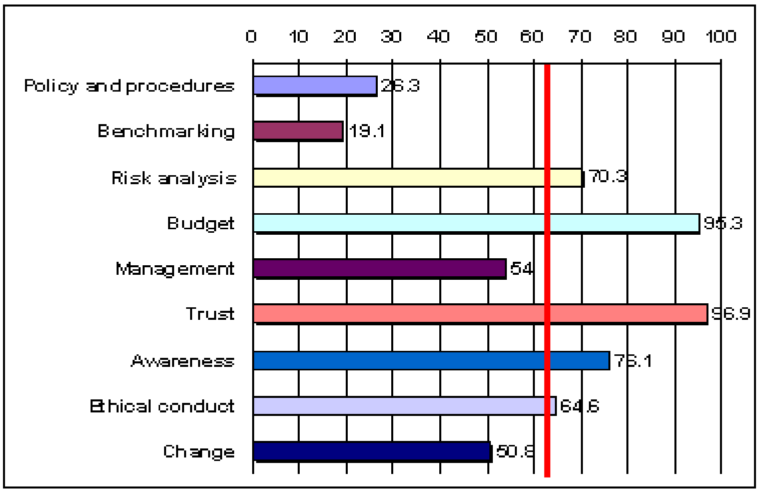


Figure 3. Sub-dimensions

The data was interpreted by considering strongly agree and agree as **positive** areas. Unsure, disagree and strongly disagree were categorised as **negative** or developmental areas. Unsure is considered as a developmental area because employees who are unsure of the use of an information security policy are not informed or aware of such a policy.

An example of the detailed findings of the sub-dimensions is reported in table 1. The left column of a table lists the statements of the sub-dimension, followed by the standard deviation and the mean for the specific statement. The standard deviation is a measure of the average of the deviations on each score from the mean [HOWE95]. The mean is the average score of the results, in other words it is the sum of the scores divided by the number of the scores [HOWE95].

Thereafter a coloured bar is given that could vary between 0% and 100%. This bar represents the percentage of respondents who felt positive or favourable about the specific statement.

Statement “a” was found to be very positive (100.0%) with a low standard deviation indicating that all respondents felt it is important to determine the organisation’s information security needs.

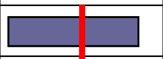
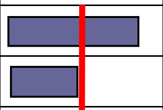
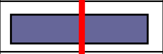
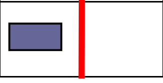
Statements	Std. dev.	Mean	Favourable percentage 0 100	Favourable
a. It is important to determine the organisation's information security needs.	0.504	4.56		100.0%
b. Information security should be regarded as a technical issue.	1.076	3.06		50.0%
c. I know what the term information security implies.	0.706	4.03		90.3%
d. Management communicates information security information on a need to know basis to all job levels.	0.878	3.06		31.3%

Table 1. Statistical data analysis

Statement "b" was perceived negatively. The high standard deviation of statement b (1.076) indicates that the distribution of responses varied between very favourable and not favourable at all. Some respondents therefore indicated that information security should be viewed as a technical issue where others felt is should not. Statement "d" indicated that most employees felt that management does not communicate information to all job levels.

4.4 Phase 4: Interpret data

The scenario of the case study indicated that there is an adequate level of information security culture at individual level and that employees are willing to secure information. At organisational and group level, however, there is a need to provide guidelines and enable employees regarding information security. The main findings were as follow:

- The organisational level was one of the critical developmental areas. Most employees were unaware of the information security policy and what was expected of them to aid in securing the organisation's information assets. This implies that the information security policy needs to be reviewed and incorporated into the working environment for the requirements to become part of the everyday activities of the employees.
- At group level, the management issue needs attention. Management needs to incorporate information security as one of the characteristics of the organisation and demonstrate its commitment to, and involvement in, the processes of implementing it effectively. Management needs to appoint a specific team or person to take responsibility for instilling the correct way in which things are done regarding information security.

- At individual level, employees need guidance in what behaviour is acceptable and what is not. The organisation needs to implement procedures such as awareness sessions and training programmes to support and communicate the information security policy from the organisational level. This will encourage employees to adhere to the information security policy, thereby instilling the correct behaviour, which is needed for an acceptable information security culture.

4.4.1 Other outcomes of the Information Security Culture Questionnaire

This scenario could vary between organisations. The information security culture assessment might indicate that there are adequate procedures and structures at both organisational and group levels. Thus, management could assist in the information security processes and provide the means for employees to adhere to the information security policy through, for instance, training. At individual level, employees might not trust management and so might not be willing to change their working practices in order to adhere to the information security policy. Trust between employees and management could also be affected by their backgrounds and nationality where their trust base might not be the same. They might also not regard ethical conduct in the working environment as important, which could result in security breaches.

These problems that could be affecting the security of information and cause people to be the weakest link in the information security chain can be identified through the information security culture assessment.

5. CONCLUSION

A certain level of information security culture is already present in every organisation using IT, but this culture could be a threat if it is not on an acceptable level. The aim in assessing that culture is to advance it to an adequate level. This could then aid in minimising internal and external threats to information in the organisation. The information security culture questionnaire can also be used to determine the results of the implementation of an information security policy or awareness campaign on the information security culture and whether employees' behaviour regarding information security actually changed.

More research is however needed to improve the current information security questionnaire. This could be done by refining the questions of the questionnaire and conducting numerous assessments at different organisations to provide a benchmark for information security culture in South Africa.

6. LIST OF RESOUCES

[BERR93] Berry, L.M. 1993. Psychology at work: An introduction to industrial and organizational psychology. Madison: Brown & Benchmark Publishers.

[DILL93] Dillon, W.R., Madden, J.T. & Firtle, N.H., 1993. Essentials of marketing research. Boston: IRWIN.

[ELOFF00] Eloff, M.M. & Von Solms S.H. 2000. Information security management: A hierarchical framework for various approaches. Computers and Security, 19(3):243-256.

[FURN93] Furnham, A. & Gunter, B. Corporate assessment: Auditing a company's personality. London: Routledge.

[MART00] Martins, E.C. 2000. Die invloed van organisasie kultuur op kreatiwiteit en innovasie in 'n universiteitsbiblioteek / The influence of organisational culture on creativity and innovation in a university library. M.Inf. Dissertation. Pretoria: University of South Africa.

[MCLU00] Mcclure, S. & Scambray, J. 2000. Security watch: Mass manipulation isn't reserved just for presidential elections: IT world be warned. InfoWorld, 22(47), November.

[ODEN97] Odendaal, A. 1997. Deelnemende bestuur en korporatiewe kultuur: onafhanklike konstrukte? / Participative management and corporate culture: independent constructs? MA. Dissertation, Rand Afrikaans University: Johannesburg.

[HELL98] Hellriegel, D., Slocum, Jr. J.W. & Woodman, R.W. 1998. Organizational Behavior. Eighth edition. South-Western College Publishing.

[HOWE95] Howell, D.C. 1995. Fundamental statistics for the behavioral sciences. Third edition. Belmont: Duxbury Press.

[PORT] The portfolio of business and management audits. Strategic Direction Publishers.

[SURV00] Survey Tracker: User's guide. 2000. OHIO, Cincinnati: Training Technologies.

[VONS00] Von Solms, B. 2000. Information security – The third wave? Computers and Security. 19(7), November: 615-620.

[WALT96] Walters, M. 1996. Employee attitude and opinion surveys. London: Institute of Personnel and Development.

[YEAT96] Yeats, D. & Cadel, J. 1996. Project management for information systems. Second edition. London: Pitman Publishing.