

A FRAMEWORK FOR EVALUATING ICT SECURITY

AWARENESS

HA Kruger, L Drevin, T Steyn

North-West University (Potchefstroom Campus)

rkwhak@puk.ac.za

+27 18 299 2539

Private Bag X6001, Computer Science and Information Systems, Potchefstroom, SA, 2520

rkwld@puk.ac.za

+27 18 299 2534

Private Bag X6001, Computer Science and Information Systems, Potchefstroom, SA, 2520

rkwts@puk.ac.za

+27 18 299 2533

Private Bag X6001, Computer Science and Information Systems, Potchefstroom, SA, 2520

ABSTRACT

ICT resources are important assets of any organization and the protection of these resources are equally important. To be able to protect themselves and their profitability, many organizations have established information security awareness programs. In order for a security awareness program to add value to an organization and at the same time make a contribution to the field of information security it is necessary to have a set of methods to study and measure its effect.

This paper gives an overview of a suggested framework for evaluating ICT security awareness. Following a brief description of the framework, a more detailed overview on the identification of areas to be evaluated, using a value focused assessment, will be presented. Comments on possible system generated information, that may be used to assist with the evaluation of security behavior of users, will also be presented.

KEY WORDS

ICT security, security awareness, value focused approach, ethics, framework, system data

A FRAMEWORK FOR EVALUATING ICT SECURITY

AWARENESS

1 INTRODUCTION

Information and information assets have become the lifeblood of organizations and the protection of these assets became one of the major aspects that management has to deal with. Often huge amounts of money and time are invested in technical solutions while the human factor receives less attention. Technical solutions are necessary to address vulnerabilities such as viruses, denial of service attacks, etc. However, the involvement of humans in information security is of equal importance and many examples of security issues such as “phising” and social engineering, where humans are involved, exist.

One of the key defences to address human-oriented controls is the implementation of an information security awareness program. These programs are used to create and maintain security – positive behavior amongst employees and the goal of such a program would be to heighten the importance of information systems security and the possible negative effects of a security breach or failure (Hansche, 2001). The importance of security awareness programs is further emphasized in the BS7799:1 where the objective of user training is given as “to ensure that all users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work”.

Following the implementation of an information security awareness program there is usually a normal business need to evaluate and measure the success and effectiveness of it. Schlienger and Teufel (2005) stated that evaluation should always be the final step in an information security management program in order to obtain information on the efficiency and effectiveness of actions, to define follow-up actions and to justify investments in the program. In an attempt to contribute to the evaluation process of an information security awareness program, this paper describes a suggested framework that may assist management with this task. The framework was developed jointly in an academic environment and at a private enterprise and it forms part of an ongoing research process. Progress to date will be highlighted – this includes an overview of the framework, the identification of areas to be evaluated using a value focused approach, and some comments on possible system generated data that may be used to assist with the evaluation of security behavior of users.

The remainder of the paper is structured as follows. Section 2 presents an overview of the proposed framework. The identification of areas to focus on is discussed in section 3 and comments on the possible use of system generated data in the process is given in section 4. Section 5 concludes the paper with some general comments.

2 PROPOSED FRAMEWORK

An initial study to develop and test a prototype model was performed during 2005 at an international mining company (Kruger and Kearney, 2005). The proposed framework in this study is based on this earlier work and some of the aspects, techniques and approaches are similar to the previous study. Briefly the suggested framework, which is presented schematically in figure 1, entails the following.

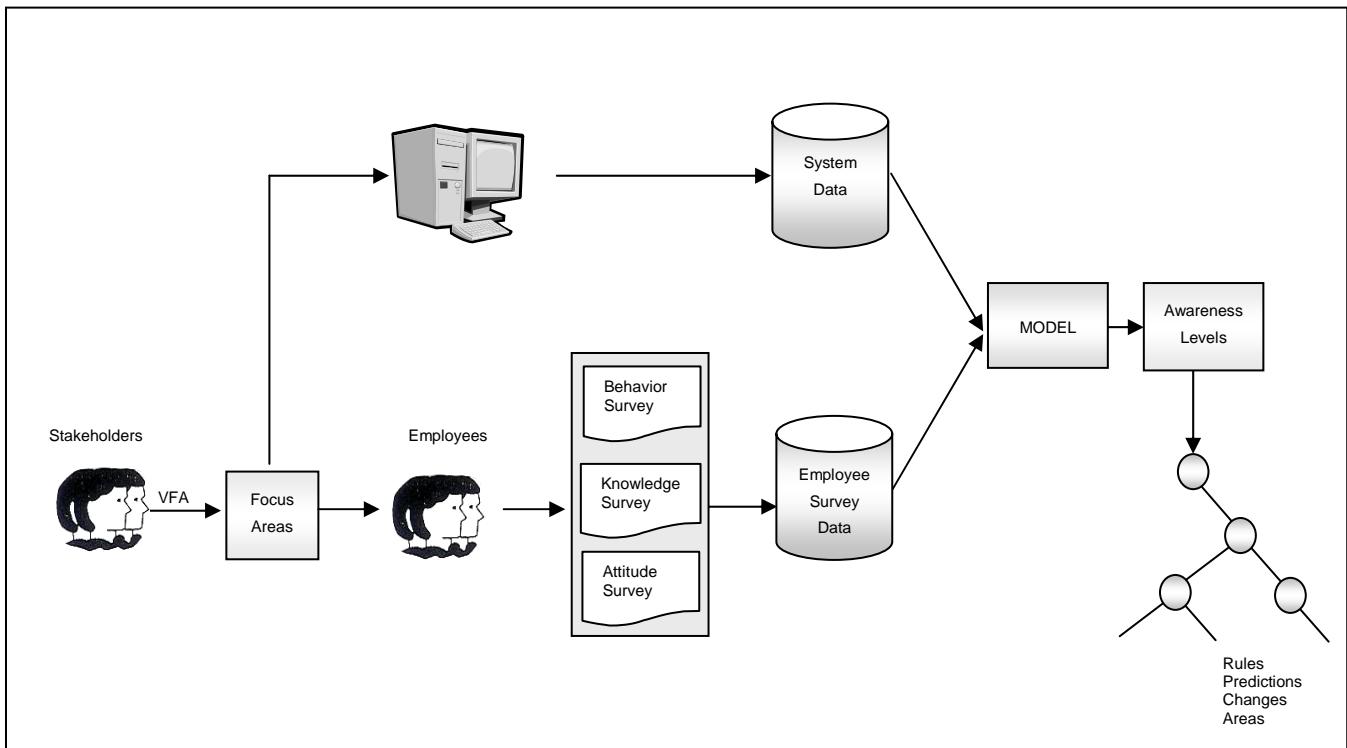


Figure 1 – Proposed Framework

As an initial step, certain areas on which measurements will be taken need to be identified. These focus areas are necessary to ensure that areas, important to all stakeholders, form the basis of a measuring tool. It will also help to focus questions, or aspects to be measured, when developing for example a survey tool. A value focused approach (VFA) that will take into account stakeholders' wishes, concerns, problems and values pertaining to information security awareness, is suggested for identifying the focus areas. This approach is presented in the next section.

Once the focus areas have been identified, employees should be surveyed to determine their level of awareness. The methodology is based on the study of Kruger and Kearney (2005) and is described by them as follows. It makes use of techniques borrowed from the field of social psychology that propose that learned predispositions to respond in a favourable or unfavourable manner to a particular object have three components: affect, behaviour and cognition. The affect component encompasses one's positive and negative emotions about something, the behaviour component consists of an intention to act in a particular manner while the cognition component refers to the beliefs and thoughts one holds about an object (Feldman, 1999; Michener and Delamater, 1994). These three components are used as a basis and the model will be developed on three equivalent dimensions namely what does a person know (knowledge); how do they feel about the topic (attitude); and what do they do (behaviour). This approach is not completely new and other researchers have already performed work where the social sciences were related to the field of information security awareness. Thomson and von Solms (1998) have shown how social psychological principles could be utilised to improve the effectiveness of an information security awareness program while Schlienger and Teufel (2003) made use of social-cultural measures to define a model for analysing information security culture in organisations.

In addition to the employee surveys, appropriate system generated data should also be used as input to the final model. This data will assist with the determination of security behaviour. System data is expected to be more reliable (not subjective or human dependent) and should be fairly easy

to get. Section 4 deals with the identification of system data and how it may be related to the focus areas.

The above data combined with appropriate importance factors will then be used to construct the final model. The model and the calculations performed will be based on aspects of value trees, score cards and other management science techniques. Details on how this is done can be found in Kruger and Kearney (2005). Using these techniques will enable decision makers to measure and present awareness levels in a drilled-down manner at different levels of detail. By applying the model at regular intervals it would be possible to measure changes in security awareness levels, focus on specific issues during follow-up security campaigns, derive rules for effective security awareness exercises and predict levels of awareness.

The ICT security and security awareness fields are dynamic and is constantly influenced by new developments and technologies. It poses ongoing challenges to both researchers and practitioners and by applying the proposed framework, a structured methodology is offered that allows for constant confirmation that the appropriate areas are addressed in an effective manner when implementing and evaluating ICT awareness programs.

3 FOCUS AREAS – A VALUE FOCUSED APPROACH

The first step in the proposed framework, in figure 1, is to identify focus areas in the security awareness domain. This was done using a value-focused approach (Drevin, Kruger and Steyn, 2006).

3.1 Methodology

The value-focused approach is a decision technique suggested by Keeney (1994) and involves four steps. First, interviews are conducted to determine stakeholders' wishes, concerns, problems etc. within the decision context. Next, the result of the interviews, which represents a list of individual values and wishes, is converted into objectives. These consist of a decision context, an object, and a direction of preference that one wants to strive towards (Nah, Siau and Sheng, 2005). Thirdly, a process to distinguish between means and fundamental objectives is performed. If an object supports or helps achieve another objective, it is classified as a means objective. Otherwise it is a fundamental objective. Finally, the means and fundamental objectives are organized into a network that shows the interrelationships among all objectives. The network can then be used to derive cause-effect relationships and to generate decision opportunities.

The value-focused thinking approach has already been applied successfully in different areas. Hassan (2004) applied it to the environmental selection of wall structures, while Nah, Siau and Sheng (2005) used the approach to describe the value of mobile applications. Other examples can be found in Dhillon and Torkzadeh (2001) and Dhillon, Bardacino and Hackney (2002) where the value-focused thinking approach was used in assessment of information system security in organizations and privacy concerns for Internet commerce respectively.

3.2 Application

Keeney's approach, as described above, was applied in an academic environment as follows.

To perform the first step, a discussion document, rather than a questionnaire, was used to obtain information from interviewees. The discussion document contained six statements or questions and was compiled according to the techniques for the identification of objectives suggested by Keeney (1994). Examples of issues discussed with interviewees include:

- What would you do or implement to increase the level of security awareness?
- What is important to you regarding ICT security awareness and how would you achieve it?

The same interview process used by Nah *et al.* (2005) was followed and interviews were conducted until no new values or objectives could be identified. A total of 7 employees were interviewed, however, no new values were obtained after the fourth interview. The interviews, which lasted for approximately one and a half hours, were recorded for future reference. Respondents included staff from both management and non-management levels and were selected from the IT department and from users. The immediate result of the interview process was a list of values that apply to ICT security awareness. These values were, in the second step, converted into objectives by changing statements such as: 'lock doors when out of office or keep laptops out of sight' into a structure consisting of a decision context, an object and a direction of preference, e.g. 'maximize physical access control'. Next, the fundamental and means objectives were derived from the list of objectives. This was done following Keeney's 'why is it important?' test. If an objective is important because it helps achieve another objective, it was categorized as a means objective; otherwise it was classified as a fundamental objective. Finally the means-ends objective network was constructed graphically by linking means and fundamental objectives to one another to show the interrelationships among them. The network is presented in Figure 2. On the left are the means objectives that show the concerns, wishes and values of the interviewees pertaining to ICT security awareness. The right hand side shows the fundamental objectives that are derived from the means objectives or stated by the stakeholders.

The fundamental objectives are in line with the acknowledged goals of ICT security e.g. integrity, confidentiality and availability. Other objectives that emerge from this exercise are more on the social and management side e.g. responsibility for actions and effective use of resources. Although no new aspects of security awareness could be identified, the approach served as confirmation that the same areas, found in any corporate environment, is important in an academic environment and could not be ignored. In addition, the results are important as the information will be used to develop a measuring instrument that will cover and focus on the identified means objectives in order to address fundamental objectives. It may also serve as a framework for management to structure an awareness program that includes all the appropriate learning areas.

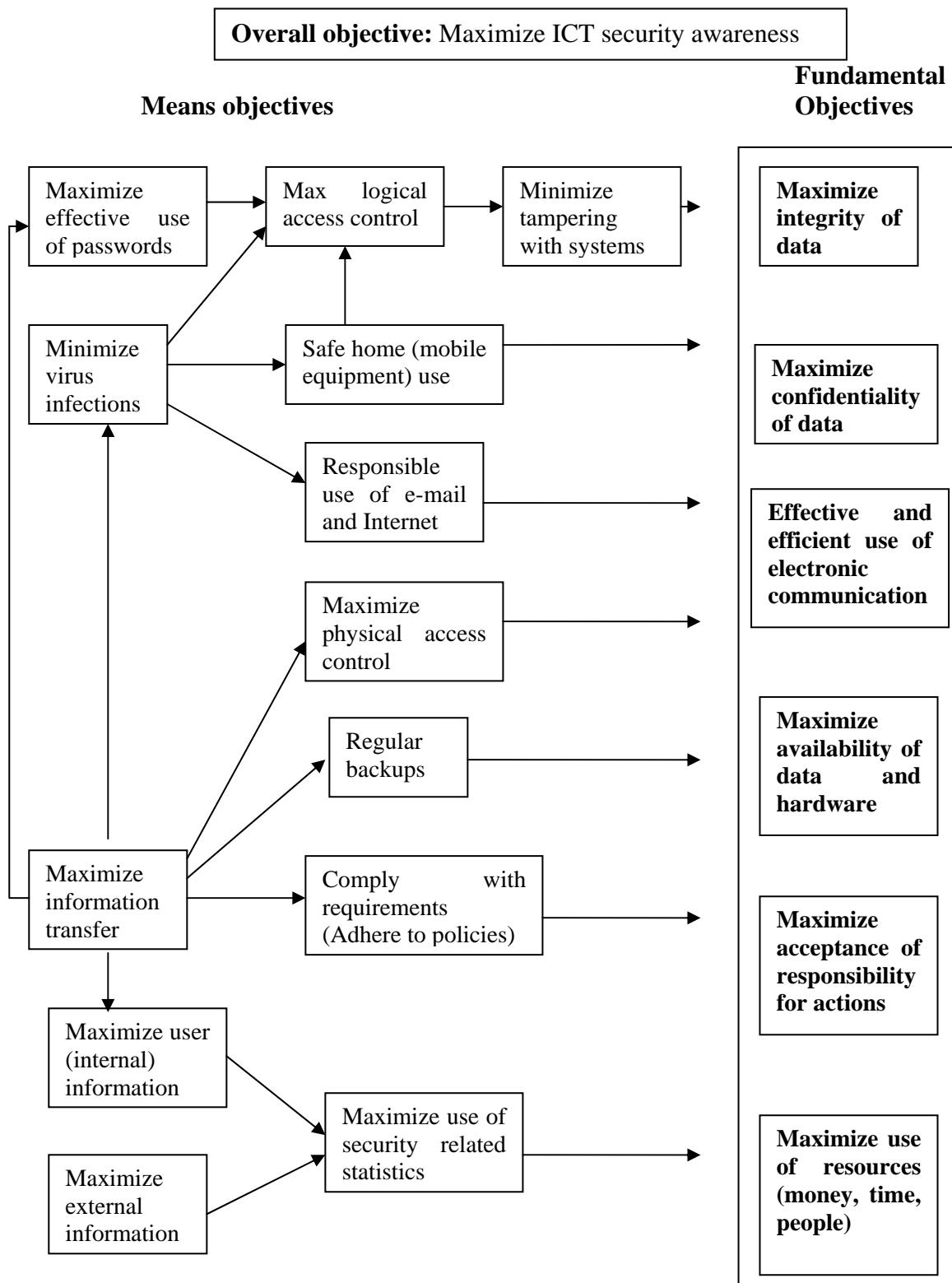


Figure 2 - Means-ends objectives network for ICT security awareness

The fundamental and means objectives derived from the network are listed in tables 1 and 2. Table 2 can be used to see what aspects influence the means objectives according to the interviewees while table 1 shows the fundamental objectives and the factors describing them.

Table 1 – Fundamental objectives

1. Maximize integrity of data
• Correctness of data; Comply with formal ICT strategy
2. Maximize confidentiality of data
• Ensure confidentiality of business, research, client (student) data
3. Effective and efficient use of e-communication systems
• Minimize cost of e-communication; Maximize e-communication resources; Minimize negative impact of e-communication
4. Maximize availability of hardware and software
• Uninterrupted usage; Prevent damage and loss
5. Maximize acceptance of responsibility for actions
• Consequences of actions
6. Maximize use of resources (money, time people)
• Comply with formal ICT strategy

Table 2 – Means objectives

1. Maximize effective use of passwords
• Use of strong passwords; Keep passwords secret; Sign off from PC when not in use; Minimize number of passwords used on the Internet
2. Maximize logical access control
• Use encryption; Limit multiple log-ins; Correct system authorizations; Separation of duties; Clean-up procedures when people resign.
3. Minimize tampering with systems
• Restricted access
4. Minimize virus infections
• Viruses from home/mobile equipment; Viruses from Internet; Viruses from e-mail
5. Safe home (mobile equipment) use
• Remote access /modems; Use of passwords
6. Responsible use of e-mail and Internet
• Cost and time for Internet usage; Handle strange e-mails with care; Large attachments; Correct defaults
7. Maximize physical access control
• Minimize theft; Use of security equipment e.g. cameras; Clean-up procedures when people resign
8. Make regular backups
• Minimize loss of data; Criteria on how long to keep data; Correct default saves; Criteria for important data; Availability of equipment to make backups
9. Maximize information transfer to employees
• Maximize IT literacy; Use communication channels (posters, bulletin boards, contracts); Criteria for important data; Illegal use of software
10. Comply with requirements (Adhere to policies)
• Make risks clear; Make security implications clear
11. Maximize user (internal) information
• Use user feedback; Use internal audit statistics; Minimize loss of knowledge e.g. when resign
12. Maximize external information
• Use external input/reports e.g. external auditors, Gartner
13. Maximize use of security related statistics
• Use all comparable statistics

4 SYSTEM INFORMATION

To complement employee surveyed data, appropriate system generated data should also be used as input into the final measuring process. System data is expected to be more reliable in certain instances as it is not human dependent. It is regarded as objective and should greatly assist in getting additional insight into the general security behaviour of ICT users. To be able to incorporate system data into the proposed model, there are three aspects that should be dealt with; technical feasibility, relevance to means and fundamental objectives and ethics.

Technical feasibility in this study simply means that the required data is available in such a form that it can be used, or that it can be extracted and transformed into usable data. The system data to be used should be related to the identified means and fundamental objectives to ensure that relevant data is obtained that can contribute to addressing stakeholders' values.

It would be possible to trace or link most of the suggested system data to specific employees. This means that there would be ethical consequences when dealing with some of the data. Traditionally ethics imply the avoidance of harm (emotionally and physically) to research subjects (employees in this study), informed consent from the research subjects to do the research and protecting the privacy and identity of the research subjects (Fontana and Frey, 2003). The ethical codes of professional bodies such as the Association for Computing Machinery and the South African Computer Society also include references to the ethical behaviour of members regarding the protection of people's privacy and confidentiality (ACM, CSSA). Confidentiality refers to an ethical principle meaning that some types of communication between a person and professionals who share the data are "privileged" and may not be discussed or divulged to third parties. Privacy is the ability of an individual or group of individuals to stop information about them from becoming known to people other than those whom they choose to give the information to. The nature of the data that needs to be gathered in this project for analysis may have significant confidentiality and privacy consequences if disclosed and linked to individual employees. It is therefore necessary to consult with the appropriate review board or ethical committee in the organization where the research project is conducted. In addition, for this study, it was decided that it would not be necessary to identify individuals or to link specific individuals to specific data. Percentages or totals of the data will suffice for analysis purposes.

For example:

- How many employees have reacted on a phising e-mail message as opposed to "who" has reacted; or
- The percentage of Internet users that surf unauthorized websites; or
- The number of users that have installed anti-virus software; or
- The percentage of users that use weak passwords.

Table 3 summarizes possible system data pertaining to the focus areas determined in section 3, which are candidates for inclusion in the model. The first column shows the system data area, the second column explains why the system data is needed, while the third one indicates the source of the data. The technical feasibility has already been cleared with IT management while the ethical aspects are still being considered.

Table 3 – System Data

System data area	Purpose	Source of data
Time spent on the Internet	Comply with policies; Availability of ICT resources	Internet logs
Illegal web page visits	Comply with policies	Internet logs; Click-stream analysis.
Passwords	Use of “strong” passwords	Tested Programmatically
Suspicious e-mail messages	Reaction of staff when dealing with suspicious e-mail that may contain viruses; responsible use of e-mail	Send out suspicious e-mail and monitor statistics on read, delete without open it, forward, etc.
Special security messages or policy announcements	Reaction of staff on security messages; comply with policies.	Send out notices and monitor statistics on read, delete without reading it, visits to web page with new policies etc.
Phising	Test attempted identity theft	Send e-mail (or use web page) and request specific information.
Installation of anti-virus software	Negative effect on availability, integrity and effective use of resources; Comply with policies; Acceptance of responsibility	System logs
Switch off PC's after hours	Unauthorised access; Spyware	System logs
Number of hits on web pages containing security policies	Comply with policies	Internet/Intranet logs
Backups on network drives	Are “personal” backups performed; Effective use of resources; Comply with policies	Network drives logs
Multiple login facilities	Unauthorised access; Comply with policies	System logs
Forwarding of chain e-mails	Availability and effective use of resources; Comply with policies	E-mail system logs
Size of e-mail attachments	Availability and effective use of resources; Comply with policies	E-mail system logs
Downloading of files from Internet e.g. huge music files	Availability and effective use of resources; Comply with policies	Internet logs
Incidents reported e.g. viruses, theft, unauthorised access etc.	Loss of data; Downgrading of performance; Physical access	Helpdesk, asset management, security department etc.
Access rights of staff that has resigned	Logical access; Integrity of data	System logs; HR department

5 CONCLUSION

In order for security awareness programs to add value to an organization and at the same time make a contribution to the field of security information it is necessary to follow a structured approach to study and measure its effect. This paper discussed a possible framework for evaluating ICT security awareness. The framework starts with the identification of areas to focus on – these areas are then used to gauge employees' knowledge, attitude and behavior levels. Combined with certain system generated data, and appropriate importance factors, the employee surveys are used as input into a model to calculate awareness levels. A discussion on the identification of focus areas was also given. To do this, a value focused approach was followed and resulted in a network of relationships that suggests how means objectives may interact and influence fundamental objectives and ultimately the overall objective of maximizing ICT awareness. Brief notes on the use of system generated data that may assist with the determination of security behavior, was also presented.

Progress and findings of the study are encouraging and the intention is to proceed with a follow-up study of the remaining phases of the proposed framework. Specific goals of the follow-up study are to (1) continue an in-depth study (currently in progress) into the availability, applicability and use of system generated data to strengthen the model, (2) generate measures representing the factors of the identified focus areas, and (3) develop a final model, using appropriate management science techniques, to generate measurements and recommendations that are reliable and valid.

Acknowledgement: Financial assistance from the National Research Foundation (NRF) is acknowledged. Opinions expressed are those of the authors.

6 REFERENCES

- ACM. Association for Computer Machinery, Code of Ethics and Professional Conduct. <http://www.acm.org/constitution/code.html#sect1>, Date used: March 2006.
- BS 7799. <http://www.thewindow.to/bs7799/4.htm>, Date used: January 2006.
- CSSA. Computer Society of South Africa, Code of Conduct. http://ethics.iit.edu/codes/coe/RSA_Code.html, Date used: March 2006.
- Dhillon, G. & Torkzadeh, G. 2001. Value-focused assessment of information system security in organizations. In: *Proceedings of the twenty second international conference on Information Systems*. 561-566.
- Dhillon, G., Bardacino, J. & Hackney, R. 2002. Value focused assessment of individual privacy concerns for Internet commerce. In: *Proceedings of the twenty third international conference on Information Systems*. 705-709.
- Drevin, L., Kruger, H.A. & Steyn, T. 2006. Value-focused assessment of ICT security awareness in an academic environment, In: *IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments*, eds. Fischer-Hubner, S., Ranneberg, K., Yngstrom, L., Lindskog, S. Boston: Springer, 448-453.
- Feldman, R.S. 1999. *Understanding Psychology*. Fifth edition. McGraw-Hill College. Boston, River Ridge, IL.
- Fontana, A. & Frey, J. H. 2003. The interview: from structured questions to negotiated text. In: Denzin N. K. & Lincoln Y. S. (Eds.), *Collecting and interpreting qualitative materials*, 61-106.

- Hansche, S. 2001. Designing a security awareness program: Part 1, *Information System Security*, January/February: 14-22.
- Hassan, O.A.B. 2004. Application of value-focused thinking on the environmental selection of wall structures, *Journal of environmental management*, 70:181-187.
- Keeney, R.L. 1994. Creativity in decision making with value-focused thinking. *Sloan Management Review*, Summer:33-41.
- Kruger, H.A. & Kearney, W.D. 2005. Measuring information security awareness: A West Africa gold mining environment case study, *In: Proceedings of the 2005 ISSA Conference, Johannesburg, South Africa, ISBN:1-86854-625-X*, 29 June – 1 July 2005.
- Michener, H.A. & Delamater, J.D. 1994. *Social Psychology*. Third edition. Harcourt Brace College Publishers. Orlando, Florida.
- Nah, F.F., Siau, K. & Sheng, H. 2005. The value of mobile applications: A utility company study. *Communications of the ACM*, 48(2):85-90.
- Schlienger, T. & Teufel, S. 2003. Information security culture – from analysis to change, *South African Computer Journal*, 31:46-52.
- Schlienger, T. & Teufel, S. 2005. Tool supported management of information security culture: An application to a private bank. *In: R. Sasaki, E.Okamoto & H. Yoshiura, Eds. The 20th IFIP International Information Security Conference (SEC 2005) – Security and Privacy in the age of ubiquitous Computing, Makuhari Messe, Chiba, Japan, Kluwer Academic Press*.
- Thompson, M.E. & Von Solms, R. 1998. Information security awareness: educating your users effectively, *Information Management & Computer Security*, 6(4):167-173.