Value-Focused Assessment of Information Communication and Technology Security Awareness in an Academic Environment

Lynette Drevin, Hennie Kruger, and Tjaart Steyn

North-West University,
Private Bag X6001, Potchefstroom, 2520, South Africa
ldrevin@acm.org, rkwhak@puk.ac.za, rkwts@puk.ac.za

Abstract. The aim of this paper is to introduce the approach of value-focused thinking when identifying information and communications technology (ICT) security awareness aspects. Security awareness is important to reduce human error, theft, fraud, and misuse of computer assets. A strong ICT security culture cannot develop and grow in a company without awareness programmes. How can personnel follow the rules when they don't know what the rules are? [1] This paper focuses on ICT security awareness and how to identify key areas of concern to address in ICT security awareness programmes by making use of the value-focused approach. The result of this approach is a network of objectives where the fundamental objectives are the key areas of concern that can be used in decision making in security planning.

1 Introduction

Employee errors are among the top ten threats to information assets according to Whitman and Mattord [2]. Security education, training and awareness are part of the process to educate staff on information security. Pfleeger and Pfleeger [3] state that people using security controls must be convinced of the need for it. They have to understand why security is important in a given situation. Cribb [1] looks at security from a business point of view and states that a single case of abuse can cause more costs than the establishment of a security system. He feels that the cost of training employees is less than the potential penalties incurred if legislation was not adhered to or the company's systems were attacked. Employees should know the rules otherwise they can't be expected to follow them. Training can prevent staff from accidentally acting inappropriately. Effective use of security controls that are in place can only be achieved when employees are aware of the need for security. BS 7799:1 has a section on user training and the objective is 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' [4].

It is necessary to do an assessment to measure the awareness of staff members regarding information communication and technology (ICT) security in general. Focus areas are necessary to measure relevant areas otherwise many aspects can be looked into without getting to the real shortcomings or issues. The value-focused

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

thinking method [5] was used in an university environment as part of a bigger security awareness project.

The aim of this paper is to introduce the approach of value-focused thinking as applied to ICT security awareness. This paper will first discuss the value-focused thinking method of arriving at fundamental objectives to identify important security awareness aspects. Next, the security awareness project will be discussed after which the results obtained will be given. A short discussion of the fundamental objectives will follow and lastly a conclusion and further research possibilities will be given.

2 Methodology: Value-Focused Thinking

Value-focused thinking is a decision technique suggested by Keeney [5]. The approach calls for the identification of the stakeholders that will be impacted by the decision. These persons or groups of persons are then questioned about their values, concerning the specific area under consideration. Their responses are then used to identify objectives. Values are those principles that one strives to and define all that one can care about in a specific situation [5]. Objectives are characterized by three features, namely: a decision context, an object and a direction of preference [6]. Keeney states that one of the greatest benefits of this approach is that better alternatives for a decision problem can be generated once objectives have been established. This is in contrast with the more traditional method, called attribute-focused thinking, where alternatives are first identified after which the objectives are specified. Following the determination of objectives, a process to distinguish between means and fundamental objectives is performed. Fundamental objectives refer to the objectives underlying the essential reasons for the problem being under consideration while means objectives are regarded as those whose attainment will help achieve the fundamental objectives [7]. Finally a means-ends objective network is constructed to show the interrelationships among all objectives. The network is then used to derive cause-effect relationships and to generate potential decision opportunities.

The value-focused thinking approach has already been applied successfully in different areas. Hassan applied it to the environmental selection of wall structures [8] while Nah, Sian and Sheng used the approach to describe the value of mobile applications [7]. Other examples can be found in Dhillon et al [9], [10] where the value-focused thinking approach was used in assessment of IS security in organizations and privacy concerns for Internet commerce. In this study the value-focused approach was applied at a university to identify key areas of concern to ICT security awareness.

3 Application of Value-Focused Thinking

Keeney's value-focused approach was used to conduct interviews and to organize the data into the required network. The primary objective of the interview process was to identify stakeholders' wishes, concerns, problems and values pertaining to ICT security awareness.

A discussion document, rather than a questionnaire, was used to obtain information from the interviewees. The discussion document contained six statements or questions and was compiled according to the techniques for the identification of objectives suggested by Keeney [5]. 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 [7] 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 were recorded for future reference. Each interview lasted approximately one and a half hours. 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 then 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, and object and a direction of preference, e.g. 'maximize physical access control'. The fundamental and means objectives were then 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 is categorized as a means objective, otherwise it is 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. A more detailed discussion on this network follows in the next section.

4 Results

A network of objectives was constructed from the data obtained during the interviews and is presented in Figure 1. 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. The results confirm that no new aspects of security awareness could be identified in an academic environment neither could any aspects be ignored. The six fundamental objectives should be addressed when planning, shaping and developing ICT security awareness programmes in order to comply with what management and users identified as crucial.

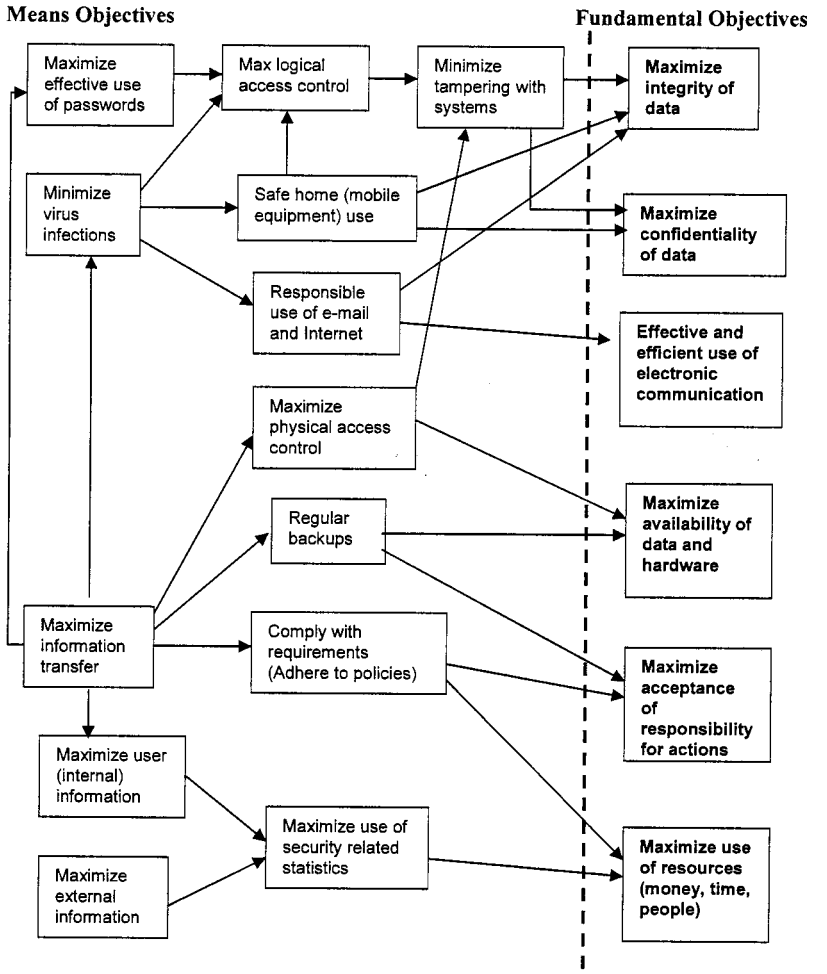

Fig. 1. Means-ends objectives network for ICT security awareness.

Overall objective: Maximize ICT security awareness to assist the university to provide a sustainable service to its staff, students and other stakeholders.

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. The value of the results is that 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 also serves as a framework for management to structure an awareness programme that includes all the appropriate learning areas.

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 password 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

5 Conclusion and Further Research

The overall objective that resulted from this phase of the project is the maximization of ICT security awareness to aid the university in providing a sustainable service to its staff, students and other stakeholders. Fundamental objectives to achieve this were identified by constructing a network using the value-focused approach. These objectives can serve as a basis for decision making and to guide the planning, shaping and development ICT security awareness in a company. ICT security awareness programmes can be used to train staff and sensitize them in the security arena to get a more secure environment compliant to standards such as BS 7799 and others.

This work is ongoing and the next step will be the formal definition and description of the objectives followed by the development of a measuring tool. The completed network will be used to develop a measuring instrument to ensure that all areas are appropriately covered. At management level the identified objectives can be used as a guideline to structure security awareness programmes.

References

1. Cribb, B. Lack of policy causes IT risks. In ITWEB. 15 Jul 2005.
2. Whitman, M.E., Mattord, H.J. Principles of Information Security. 2nd edn. Thomson (2005).
3. Pfleeger, C.P., Pfleeger, S.L. Security in Computing. 3rd edn. Prentice Hall (2003).
4. BS 7799. http://www.thewindow.to/bs7799/4.htm. Used on 31 Oct 2005.
5. Keeney, R.L. Creativity in decision making with value-focused thinking. Sloan Management Review, Summer (1994) 33-41.
6. Sheng, H., Nah, F.F., Siau, K. Strategic implications of mobile technology: A case study in using value-focused thinking. Journal of Strategic Information Systems. (2005) 1-22 (Article in press).
7. Nah, F.F., Siau, K. & Sheng, H. The value of mobile applications: A utility company study, Communications of the ACM, 48(2). (2005) 85-90.
8. Hassan, O.A.B. Application of value-focused thinking on the environmental selection of wall structures, Journal of environmental management, 70. (2004) 181-187.
9. Dhillon, G., Torkzadeh, G. Value-focused assessment of information system security in organizations. Proceedings of the twenty second international conference on Information Systems. (2001) 561-566.
10. Dhillon, G., Bardacino, J., Hackney, R. Value focused assessment of individual privacy concerns for Internet commerce. Proceedings of the twenty third international conference on Information Systems. (2002) 705-709.