# MEASURING INFORMATION SECURITY AWARENESS:

# A WEST AFRICA GOLD MINING ENVIRONMENT CASE STUDY

HA Kruger[1] and WD Kearney[2]

[1]School of Computer-, Statistical- and Mathematical Sciences, North-West University (Potchefstroom Campus)

[2]AngloGold Ashanti, Perth, Australia

[1]rkwhak@puknet.puk.ac.za, 018 2992539, Private Bag X6001, POTCHEFSTROOM, 2520

[2]wkearney@anglogoldashanti.com, 08 94254621, Level 13, St. Martins Tower, PERTH WA 6000

## ABSTRACT

AngloGold Ashanti is an international gold mining company that has recently implemented an information security awareness program worldwide at all of their operations. Following the implementation, there was a normal business need to evaluate and measure the success and effectiveness of the program. A measuring tool that can be applied globally and that addressed AngloGold Ashanti's unique requirements was developed and applied at the mining sites located in the West Africa region. The objective of this paper is, firstly, to give a brief overview on the measuring tool developed and, secondly to report on the application and results in the West Africa region.

KEY WORDS
Information security; Information security awareness; Quantitative modelling; Case study.

# MEASURING INFORMATION SECURITY AWARENESS:
# A WEST AFRICA GOLD MINING ENVIRONMENT CASE STUDY

## 1 INTRODUCTION

AngloGold Ashanti is a global African gold producer with 25 operations in 11 countries and is listed on a number of stock exchange markets such as the JSE Securities Exchange, NYSE etc. Over 6 million ounces of gold are produced annually and it has one of the world's largest reserves and resources bases and focused exploration activities around the globe. The company employs more than 62 500 people around the world.

Like every other organisation using information technology, AngloGold Ashanti faces an internal and external threat in terms of information risk. It was however clear that, in an organisation of this size and diverse locations of operations, there was no clean and simple answer to creating an effective and secure information environment. It was realized by senior management that one of the key aspects would be to raise the general level of information security awareness and to educate all computer users in the basics of information security. One of the first steps in this challenge was to create an awareness of the risks and then to ensure that these risks are managed. The initial aim or objective was to ensure that the AngloGold Ashanti computer users are aware of the risks associated with using information technology as well as understanding and abiding by the policies and procedures that are in place.

To achieve this, an information security awareness program was started in the last quarter of 2003. The program was focussed on six critical risk areas or ‘golden rules’:

- Always adhere to AngloGold Ashanti policies
- Keep passwords and personal identification numbers (PINs) secret
- Use e-mail and the Internet with care
- Be careful when using mobile equipment
- Report incidents like viruses, thefts and losses
- Be aware, all actions carry consequences

The program was rolled out to all computer users and entails presentations (including a video), brochures, posters, web information, and articles in in-house magazines etc. All material was made available in English, Spanish, French and Portuguese.

Following the implementation of the program there was a normal business need to evaluate and measure the success and effectiveness of it. A comprehensive measuring tool that can be applied globally and that will address AngloGold Ashanti’s unique requirements at the different operations was needed to sustain the program. To this end, a prototype model to measure the information security awareness levels at AngloGold Ashanti was developed during 2004 and applied to the company’s operational sites in Ghana in West Africa to obtain a baseline measurement. The purpose of this paper is to give a brief overview on the measuring tool developed and to report on the application and results of the baseline measurement in Ghana.

The remainder of the paper is organised as follows. Section 2 briefly provides background on the measurement tool and the methodology followed in the application. Section 3 gives an overview of the results while section 4 highlights issues to consider for future use of the tool. Section 5 concludes the paper with some general comments.

## 2 BACKGROUND

The methodology used to develop the measuring tool was based on 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 were used as a basis and the model was 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.

To develop a measuring tool and perform the actual measurements, two distinctive challenges were identified: what to measure and how to measure it. Requirements such as sustainability, ease of use, the use of scientific methods and complying with the organisation's unique requirements, all added to the challenge of finding a suitable methodology to create the measuring tool with. It was decided to measure the three dimensions knowledge (what you know), attitude (what you think) and behavior (what you do). Each one of these dimensions was then subdivided into the six focus areas discussed in section 1 and on which the awareness program was based. Where appropriate and through consensus the six focus areas were further subdivided into specific factors, for example, the focus area Passwords was broken down into two subcategories *Purpose of passwords* and *Confidentiality of passwords*. Confidentiality of passwords was then further broken down into *Writing down of passwords* and *giving passwords to others*. To assist in the problem structuring process a hierarchy of criteria was identified using a tree structure. This process is often referred to as a value tree and a complete discussion of value trees, how they are constructed and used, can be found in Belton and Stewart (2002).

An illustration of the tree structure developed is shown in figure 1.

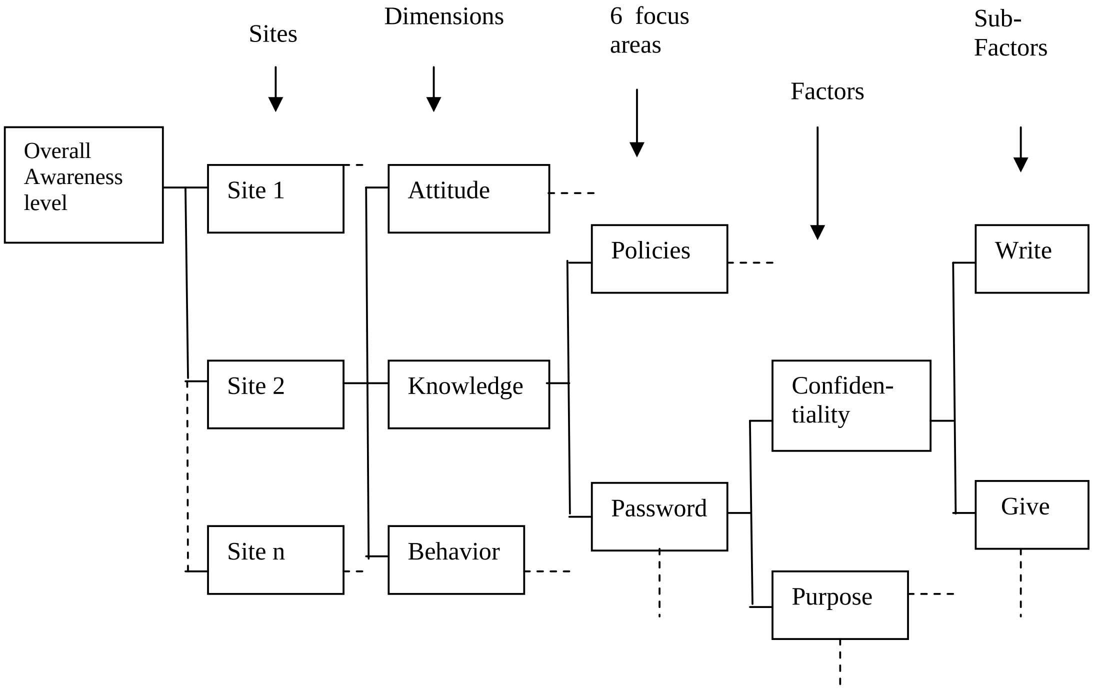


***Figure 1 – Tree structure of problem***

The use of a value tree suggests solving the tree in a backward manner i.e. the tree is solved from the lowest level working upwards through the different levels. This was done using a simple scorecard approach defined as $V(a)=\sum_{i=1}^{n} v_i(a)w_i$ where V(a) is the overall value of alternative a, $v_i(a)$ is the value score reflecting alternative a's performance on criterion i and $w_i$, the weight assigned to reflect the importance of criterion i. This additive model is one of the most widely used forms of a value function and is described in detail in Belton and Stewart (2002).

The performance, $v_i(a)$, was determined using a questionnaire. Thirty-five questions were designed to test the knowledge, attitude and behaviour of respondents pertaining to the six main focus areas and their factors and sub-factors. Some of the questions were answered on a 3-point scale – true, don't know and false, while others only needed a true or false response. This way of measuring how respondents may act is in line with methods suggested in social psychology (Michener and De Lamater, 1994) and agrees with methods used and proposed by other researchers and practitioners in the field of information security awareness e.g. Pentasafe's security awareness report (Pentasafe, 2002), Schlienger and Teufel (2003), Teare and Da Veiga (2003) and Martins en Eloff (2001). Figure 2 shows an example of a question in each of the three dimensions.

Example question to test *knowledge*:
Internet access on the company's systems is a corporate resource and should be used for business purposes only **1. True 2. False 3. Do not know**

Example question to test *attitude*:
Mobile equipment is usually covered with existing insurance cover and there is no special need to include them in security policies **1. True 2. False 3. Do not know**

Example question to test *behaviour*:
I am aware that you should never give your password to somebody else – however, my work is of such a nature that I do give my password from time to time to a colleague (only to those that I trust!) **1. True 2. False**

***Figure 2 – Example questions***

If necessary, the measuring process can be supported by physical tests to verify actual behaviour and internal audit departments may be a valuable source of help in this regard.

The importance weights, $w_i$, was determined using the Analytic Hierarchy Process (AHP). The AHP approach makes use of pair-wise comparisons to provide a subjective evaluation of factors based on management's professional judgment and opinion. The comparisons are made using a preference scale, which assigns numerical values to different levels of preference. A square matrix is then derived from the pairwise comparisons and a scale is extracted based on the matrix's eigenvector associated with the largest eigenvalue. When this vector is normalised to sum to one, the solution is unique and represents a numerical measure of the decision maker's perceptions of the relative importance of criteria. A consistency index can then be computed to measure the degree of inconsistency in the pairwise comparisons. TL Saaty developed the AHP and a good description of the technical details and application possibilities can be found in Saaty (1980) and Vargas (1983). A comprehensive literature review of AHP applications in different fields and areas can also be found in Vaida and Kumar (in press).

During November 2004, the model was applied to AngloGold Ashanti's West African region to obtain a baseline measurement. The West African region of AngloGold Ashanti, with its regional head office located in Accra, has four operating mines, three in Ghana and one in Guinea. Collectively these four mines employs about 10 000 people. Over 600 000 ounces of gold was produced in 2004 by the West African region.

The data capturing (questionnaire) part of the prototype tool was converted into a web-based questionnaire and made available to certain information technology users at the four mines and the regional office in Accra. Where necessary, the questionnaire was translated into French to ensure a broader coverage. Sixty-eight responses were received and these were used as input into the model. The Information Security Manager, responsible for the organization's global information security, provided the pairwise comparisons to calculate the importance weights. The ideal is that the importance weights be based on input from all relevant managers – this will be considered as part of an ongoing research project.

## 3 RESULTS

To compute the final measurements, the following weights and awareness scale were used.

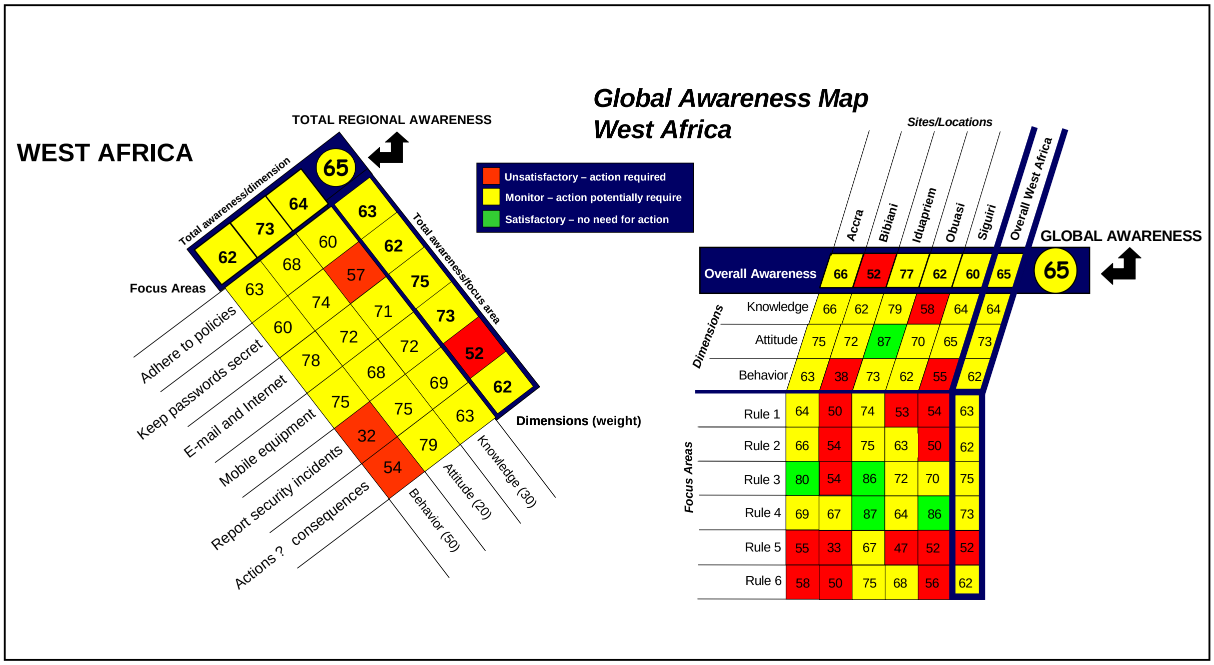
| Dimensions | Weightings |
|---|---|
| Knowledge | 30 |
| Attitude | 20 |
| Behaviour | 50 |

| Rules | Weightings |
|---|---|
| Adhere to policies | 20 |
| Keep passwords secret | 20 |
| Use e-mail/Internet with care | 20 |
| Careful with mobile equipment | 10 |
| Report security incidents | 10 |
| Actions carry consequences | 20 |

The reporting purposes, the following awareness scale was used:

| | | |
|---|---|---|
| Good (80% - 100%) | 🟩 | Satisfactory – no need for action |
| Average (79% - 60%) | 🟨 | Monitor – action potentially required |
| Poor (59% and less) | 🟥 | Unsatisfactory – action required |

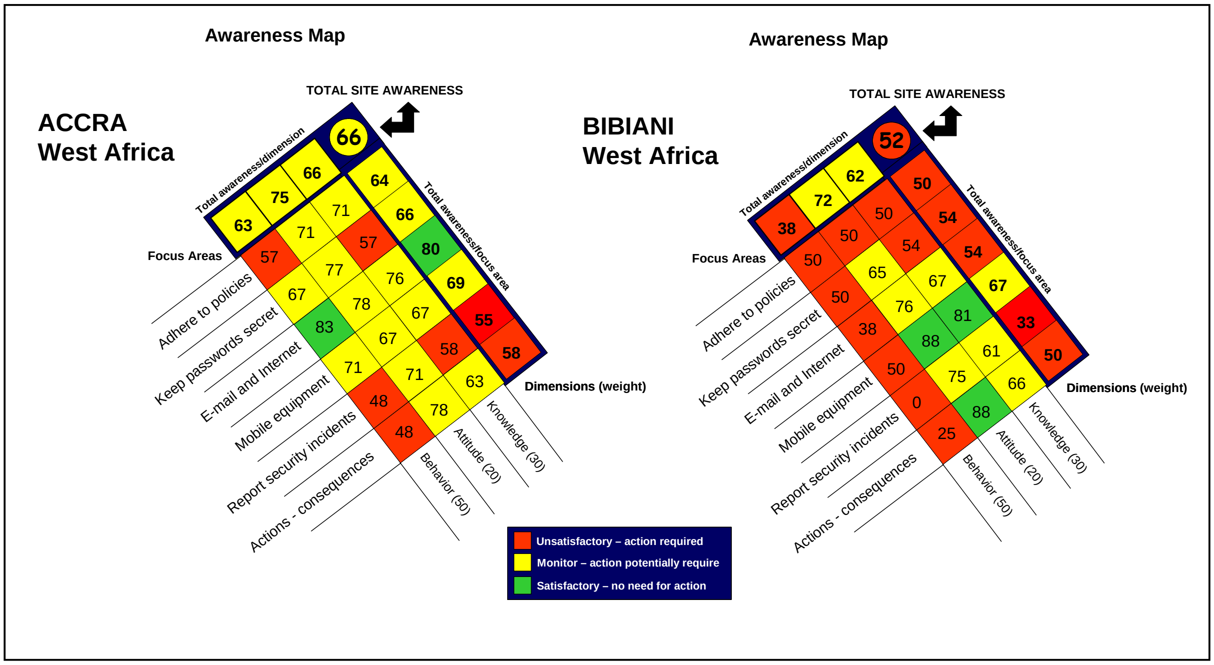
A colour-coded regional 'awareness map' - see figure 3(a) - was used to present the results and findings of the project. The colour codes give immediate information on which areas are satisfactory, should be monitored or need immediate attention. Having produced a regional awareness map for each site, a 'Global Awareness Map', consisting of the awareness levels in each site, was constructed to show the breakdown of the global awareness level. Colour codes were again added to facilitate the direction of new or changed awareness campaigns to those dimensions and/or focus areas that did not measure satisfactorily. Figure 3(b) shows the global awareness map. Figure 4 shows the awareness maps for two of the five sites.



| Focus Areas | Knowledge (30) | Attitude (20) | Behavior (50) | Total awareness/focus area |
|---|---|---|---|---|
| Adhere to policies | 60 | 68 | 63 | 63 |
| Keep passwords secret | 57 | 74 | 60 | 62 |
| E-mail and Internet | 71 | 72 | 78 | 75 |
| Mobile equipment | 72 | 68 | 75 | 73 |
| Report security incidents | 69 | 75 | 32 | 52 |
| Actions ? consequences | 63 | 79 | 54 | 62 |
| Total awareness/dimension | 64 | 73 | 62 | 65 |

| | Accra | Bibiani | Iduapriem | Obuasi | Siguiri | Overall West Africa |
|---|---|---|---|---|---|---|
| Overall Awareness | 66 | 52 | 77 | 62 | 60 | 65 |
| Knowledge | 66 | 62 | 79 | 58 | 64 | 64 |
| Attitude | 75 | 72 | 87 | 70 | 65 | 73 |
| Behavior | 63 | 38 | 73 | 62 | 55 | 62 |
| Rule 1 | 64 | 50 | 74 | 53 | 54 | 63 |
| Rule 2 | 66 | 54 | 75 | 63 | 50 | 62 |
| Rule 3 | 80 | 54 | 86 | 72 | 70 | 75 |
| Rule 4 | 69 | 67 | 87 | 64 | 86 | 73 |
| Rule 5 | 55 | 33 | 67 | 47 | 52 | 52 |
| Rule 6 | 58 | 50 | 75 | 68 | 56 | 62 |

*Figure 3(a)* *Figure 3(b)*



| ACCRA Focus Areas | Knowledge (30) | Attitude (20) | Behavior (50) | Total awareness/focus area |
|---|---|---|---|---|
| Adhere to policies | 71 | 71 | 57 | 64 |
| Keep passwords secret | 57 | 77 | 67 | 66 |
| E-mail and Internet | 76 | 78 | 83 | 80 |
| Mobile equipment | 67 | 67 | 71 | 69 |
| Report security incidents | 58 | 71 | 48 | 55 |
| Actions - consequences | 63 | 78 | 48 | 58 |
| Total awareness/dimension | 66 | 75 | 63 | 66 |

| BIBIANI Focus Areas | Knowledge (30) | Attitude (20) | Behavior (50) | Total awareness/focus area |
|---|---|---|---|---|
| Adhere to policies | 50 | 50 | 50 | 50 |
| Keep passwords secret | 54 | 65 | 50 | 54 |
| E-mail and Internet | 67 | 76 | 38 | 54 |
| Mobile equipment | 81 | 88 | 50 | 67 |
| Report security incidents | 61 | 75 | 0 | 33 |
| Actions - consequences | 66 | 88 | 25 | 50 |
| Total awareness/dimension | 62 | 72 | 38 | 52 |

*Figure 4*

It is easy to see from the awareness map in figure 3(a) that:

- The **overall awareness** level in the West African Region was measured as 65%. This is an **average** level and indicates that the awareness level should be monitored.
- The total awareness level for each one of the three **dimensions** (knowledge, attitude and behavior) was measured as an **average**.

- The total awareness level for the following five rules was measured as an **average**; **Policies, Passwords, E-mail/Internet, Mobile equipment** and **Actions carry consequences.**
- The total awareness level for the rule **“Report security incidents”** was measured as **unsatisfactory.**

The results summarized in the awareness map suggest that the following areas would require priority focus.

- **Report security incidents**

  To achieve a higher level of awareness, the **behavior** dimension (32%) should receive attention. In general, employees answered that they would not formally report security incidents although they would make an effort to resolve security problems. Aspects that need attention is that employees should be made aware of what constitutes a security incident and when and where these incidents should be reported.

- **Keep passwords secret**

  Both the **behavior** (60%) and **knowledge** (57%) dimensions should receive attention. The main problem with the behavior (maybe as a result of lack of knowledge) is that employees admit that they do write their passwords on pieces of paper to help remind them. Apparently, they are also willing to give their passwords to others, if so requested.

- **Actions carry consequences**

  Both the **behavior** (54%) and **knowledge** (63%) dimensions should receive attention. An interesting observation was that only 75% of respondents believe that they would not be held accountable if someone else uses their workstations for illegal purposes. About half of the respondents do not take any precautionary steps to prevent possible negative consequences of actions, e.g. to have a simple backup schedule or plan for information that is not automatically backed-up.

It was interesting to note that there are a number of issues where the respondents’ general attitude was very positive (see attitude in awareness map), but they do not believe that these “positive things” are being practiced at their own company or that it is applicable to them. Some examples include the following. Respondents believe that in general all attachments to e-mails should be scanned for viruses, while they do not believe that this applies to their company – their perception is that only non-business attachments are scanned. Respondents believe that in general mobile equipment should be covered in security policies, even though they are also covered by existing insurance. In the case of AngloGold Ashanti their perception is that mobile equipment does not form part of security policies because they are already covered by existing insurance. Respondents believe that in general passwords should not be written on a piece of paper or given to supervisors, while they state that this does happen at their place of work.

Another interesting observation, which was softened by the combined effect of questions and importance weightings, was that employees believe that Management or the IT department is responsible for complying with policies and even for the responsible use of the Internet. They do not know that the responsibility lies, in the first instance, with them. This is a general knowledge problem.

## 4 FUTURE DEVELOPMENT

The results obtained are promising in the sense that they are based on sound data capturing and processing techniques, easy to prepare and present and easy to understand. To gain the full benefit of the model there are a couple of aspects that may be considered for change/enhancement. The following is being considered as part of an ongoing research project.

i. The model should be applied in the other Regions as well to obtain an overall awareness level for AngloGold Ashanti.

ii. Measuring at each region should be repeated after a certain period of time (e.g. 12 or 15 months). This will facilitate the monitoring of change in security behavior and assist with business decisions such as the revision or repeating of security awareness programs.

iii. The model can be further refined to enhance the process and to provide even more accurate measurements. Examples of enhancements may include:

    - Full automation of the complete process (data capturing, processing of data and reporting facilities) – most of the processing and interpretation currently requires manual intervention
    - Development of new/additional questions to prevent "learning" of answers by respondents
    - Method to randomly select questions for each application of the model
    - Using system data as input in certain cases (as opposed to ask questions to staff)
    - A more sophisticated way of evaluating respondents' answers, e.g. the use of a 5-point scale.

## 5 CONCLUSION

There are numerous reasons why organisations have to spend effort and resources on the evaluation or measurement of information security awareness successes. Posthumus and Von Solms (2004) motivated the need to integrate information security into corporate governance and proposed a framework to aid organisations in their integration efforts. The importance of an information security awareness-measuring tool can therefore - apart from reasons such as return on investment, re-directing of security campaigns etc. – also be linked to the highest management level in an organisation. Information security has much to do with management and aspects, such as directing and controlling, are important. These aspects are functions of the Board of Directors of a company and for them to fulfill their role and have a proper corporate and information security governance framework in place; they need feedback on what is happening in the company in terms of information security. The awareness measurement tool, developed in this study, may assist a great deal in providing feedback to the Board of Directors on the success of an information security awareness program, and will assist them in their function of controlling and directing strategic objectives set for information security.

Having implemented an information security awareness program does not automatically guarantee that all employees understand their role in ensuring the security and safeguarding of information and information assets. In order for security awareness programs to add value to an organisation and at the same time make a contribution to the field of information security it is necessary to follow a structured approach to study and measure its effect.

This paper described the development and application of a prototype to measure information security awareness at an international gold mining company. The model makes use of a simple data gathering process and weighting system and, combined with certain multi-criteria problem solution techniques, provides a quantitative measurement of security awareness levels. It is based on the sound principles of sustainability, sophistication and scientific validity and could be used as a basis for a more comprehensive and sophisticated measuring system. The model was successfully applied to one of the regions of the company and a strong foundation for further use has been laid. Several opportunities for enhancement exist and some of these aspects are currently considered to improve the model, e.g. the use of a 5- or 7-point Likert-type scale to evaluate questions, a more user-friendly system to derive importance weights etc.

## REFERENCES

Belton, V & Stewart, T.J. 2002. *Multiple criteria decision analysis. An integrated approach.* Kluwer Academic Publishers. Dordrecht.

Feldman, R.S. 1999. *Understanding Psychology.* Fifth edition. McGraw-Hill College. Boston, River Ridge, IL.

Martins, A. & Eloff, J.H.P. 2001. Measuring information security. http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Martins.pdf. Date used: August 2004.

Michener, H.A & Delamater, J.D. 1994. *Social Psychology.* Third edition. Harcourt Brace College Publishers. Orlando, Florida.

Pentasafe. 2002. *Security Awareness Index Report: The state of security awareness among organisations worldwide.* Pentasafe Security Technologies, 55p.

Posthumus, S. & Von Solms, R. 2004. A framework for the governance of information security, *Computers and Security,* 23(8):638-646.

Saaty, T.L. 1980. *The analytic hierarchy process.* McGraw-Hill.

Schlienger, T. & Teufel, S. 2003. Information security culture – from analysis to change, *South African Computer Journal,* 31:46-52.

Teare, G. & Da Veiga, A. 2003. Information security culture and awareness, *Paper presented at the 2003 ISSA Conference, Sandton Convention Centre, South Africa,* 9-11 July 2003.

Thompson, M.E. & Von Solms, R. 1998. Information security awareness: educating your users effectively, *Information Management & Computer Security,* 6(4):167-173.

Vaida, O.S. & Kumar, S. 2004. Analytic hierarchy process: An overview of applications, *European Journal of Operational Research,* 2004, Article in Press.

Vargas, L.G. & Dougherty, J.J. 1982. The analytic hierarchy process and multicriterion decision making, *American Journal of Mathematical and Management Sciences,* 19(1):59-92.