available at www.sciencedirect.com

SCIENCE DIRECT®

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# A prototype for assessing information security awareness

*H.A. Kruger*[a,*], *W.D. Kearney*[b,1]

[a]*School of Computer-, Statistical- and Mathematical Sciences, North-West University (Potchefstroom Campus), Private Bag X6001, Potchefstroom 2520, South Africa*
[b]*AngloGold Ashanti, Level 13, St Martins Tower, 44, St Georges Terrace, Perth WA 6000, Australia*

ARTICLE INFO

*Article history:*
Received 19 January 2005
Revised 22 December 2005
Accepted 6 February 2006

*Keywords:*
Information security awareness
Quantitative modelling
Knowledge
Attitude
Behaviour

ABSTRACT

Due to the intensified need for improved information security, many organisations have established information security awareness programs to ensure that their employees are informed and aware of security risks, thereby protecting themselves and their profitability. In order for a security awareness program to add value to an organisation 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. The objective of this paper is to report on the development of a prototype model for measuring information security awareness in an international mining company. Following a description of the model, a brief discussion of the application results is presented.



## 1. Introduction

Security risks associated with information technology are a topic that has become increasingly significant. As corporations rely ever more on technology to run their businesses, security is becoming a major concern rather than an afterthought. The CERT Co-ordination Center at Carnegie Mellon University has reported that security incidents, reported security attacks that may involve one site or thousands of sites, have increased by 68% from 2003 to 2004 (CERT/CC, 2004).

Whilst information security generally focuses on protecting the confidentiality, integrity and availability of information, information security awareness deals with the use of security awareness programs to create and maintain security-positive behaviour as a critical element in an effective information security environment. According to Hansche (2001: p. 14) the goal of a security awareness program is to heighten the importance of information systems security and the possible negative effects of a security breach or failure. The Information Security Forum (ISF, 2003) defines information security awareness as the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organisation, their individual security responsibilities, and acts accordingly.

The effective management of information security requires a combination of technical and procedural controls to manage information risk. The value of controls usually depends on the people implementing and using them and in information security that is no different. Controls can be circumvented or abused by employees who ignore security policies and procedures. The implementation of effective security controls is thus dependent upon the creation of a *security positive environment*, where everyone understands and engages in the behaviours that are expected of them. See for example Von Solms and Von Solms (2004) who offered

* *Corresponding author*. Tel.: +27 18 2992539; fax: +27 18 2992570.
E-mail addresses: rkwhak@puknet.puk.ac.za (H.A. Kruger), wkearney@anglogoldashanti.com (W.D. Kearney).
[1] Tel.: +61 8 94254621; fax: +61 8 94254650.

0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.02.008

guidelines on how to move from information security policies to a positive information security culture. The change to a security positive environment or culture is, however, not always easy and straightforward. The ISF's Information Security Status Survey (ISF, 2002) indicated that most members believe that the effectiveness of their security awareness initiatives does not rate especially highly, and that more than four out of five feel they do not commit sufficient time and resources to their awareness activities. In a similar vein, a recent computer crime and security survey (CSI, 2004) found that the vast majority of the organisations in the review view information security awareness training as important, though (on average) respondents from all sectors do not believe their organisations invest enough in this area.

There appears to be sufficient material to help organisations with delivering a proper security awareness program and what to do to influence employees positively, e.g. Information Technology – Code of Practice for Information Security Management (ISO 17799, 2000), The Standard of Good Practice for Information Security (ISF, 2003), Leach (2003), Furnell et al. (2002), Hansche (2001) and Spurling (1995). There is, however, a lot less available in the literature on how to measure the effectiveness of these programs. Pentasafe Security Technologies (Pentasafe, 2002) produced a comprehensive security awareness report that was based on responses from 1348 workers and 583 organisations worldwide. It represents a major effort to measure how organisations improve security awareness and how well employees understand and act upon information security policies, threats and issues in their respective organisations. Examples of other information security measurement aspects can be found in Martins and Eloff (2001) who suggested that the measurement of information security management should be performed on two levels, viz. a business and management process level and a technical level; Stanton et al. (2005) presented work on the systematical classification of information security end user behaviours that could be used when analysing (measure) security behaviour.

Information security awareness is a dynamic process, made even more difficult in that risks continuously change. As a result, any awareness program needs to be continually measured and managed to keep abreast of changes in risk profiles. To keep the users current and their memories refreshed, any awareness program must be ongoing and be an integral part of the very culture of the enterprise. The key to success in awareness is keeping the messages relevant and consistent, while varying the delivery mechanisms, to keep everyone interested. Both the delivery mechanism and the risk areas could change as the information risk profile changes. Schlienger and Teufel (2003) discuss this where awareness and training programs lead from ''become aware'' to ''stay aware'' and ends up in ''be aware'', which changes a security culture definitively. To address the issue of continuous change and measurement of information security awareness, a project was initiated at an international gold mining company to investigate the feasibility of developing a measurement model. The goal of the model, which forms part of an ongoing research project, was to monitor change in security behaviour and as a result revise or repeat security awareness campaigns.

The remainder of this paper is organised as follows. Section 2 briefly introduces the international gold mining company where the study was performed. Section 3 describes the methodology used while Section 4 deals with an application of the model, the modelling results and recommendations. Section 5 concludes the paper with some general comments.

## 2. Background

An international gold mining company, which recently implemented a security awareness program worldwide at all their operations agreed to assist with the research project. The company is a global African gold producer with 25 operations in 11 countries and has gold production of over 6 million ounces annually. The company was formed in 2004 out of the merging of two existing gold mining companies. The merged company has one of the world's largest reserves and resource bases and focused exploration activities around the globe. Employing more than 62,500 people around the world, the company is listed on the following exchanges: JSE Securities Exchange, NYSE, ASX, LSE, GSE and the Euronext Paris and Euronext Brussels.

In an organisation of this size and diverse locations of operations, it was clear that there is no silver bullet or clean and simple answer to create an effective and secure information environment. The management of the risk in this fluid and dynamic environment involves significant expenditure together with an ongoing business and information technology partnership. The company, like every other organisation using information technology, faces a real internal and external threat in terms of information risk. Information security apathy and ignorance are some of the biggest threats to computer systems and a significant and lasting improvement in information security will not be achieved by throwing more technical solutions and sophisticated processes at the problem – it is by raising the general level of information security awareness and educating all computer users in the basics of information security. One of the first steps in this challenge was then to create an awareness of the risks and then to ensure the risk is managed. The initial aim or objective was to ensure that 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 initiated. Briefly the program involved the following. A comprehensive toolkit was purchased from a vendor and detailed development of the program started in mid-2003. The first priority was to narrow the focus of the program into a manageable size. After careful deliberation and following a risk elimination process, the program was focused on six critical risk areas or 'Golden Rules', the first five being:

- Always adhere to company 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

The last is the heart of the program, namely *Be aware, all actions carry consequences* – once again, back to the people issue.

The toolkit purchased, consisted of a complete awareness solution, and it was decided to use only those portions relevant to the specific needs of the company and to customise other areas to suit specific needs. The program was rolled out to all computer users, not all employees.

The program was developed as follows:

- Basic presentation to all computer users, including a video, not longer than an hour
- Brochures to all participants
- Different posters put up in all regional offices and Business Units
- Website with all details, including ''Ask a question'' option available on the global Intranet
- Articles in the company's in-house magazine

Presentations were geared towards different audiences, with a similar core message but delivered to suit the audience. The video was customised with the company's logo and name, as well as digital images of Business Units, staff members and corporate office. The video has been translated into French, Spanish and Brazilian Portuguese, together with UK, Australian, South African and American English versions. While it may seem excessive, it was very important to get the local buy-in and identification with the program. Presentations, posters and brochures were in English, Spanish, French and Portuguese.

Following the implementation of the program there was a need to evaluate and measure the success and effectiveness of it. The purchased toolkit contains a basic measuring tool based on multiple-choice questions that a respondent has to answer. The number of right answers is then used as an indication of the awareness in a certain region. There was, however, a need for a more comprehensive measuring tool that can be applied globally and that will address the company's unique requirements at the different operations.

## 3. Methodology

The methodology used to develop the measuring tool was based on techniques borrowed from the field of social psychology that proposes 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, the researcher or decision maker is confronted with two distinctive challenges: what to measure and how to measure it. In this study, requirements such as sustainability, ease of use, the use of scientific methods and complying with the organisation's unique requirements, all add to the challenge of finding a suitable methodology to create the measuring tool with.

### 3.1. *What to measure*

A global information security awareness level for the organisation was the main measurement required. To achieve this, it would be necessary to measure awareness levels at each region and then in a meaningful way combine those regional levels into an overall measurement.

It was agreed that one ''set of aspects'' would be measured at all the regions although they might not be of equal importance in all the regions – importance was handled through a weighting system which is discussed later on. This approach called for the identification of key factors that would form the basis of the evaluation. 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, which is a simple representation, capturing the essence of a problem, extracted from a complex problem description and can be constructed by using either a top-down or bottom-up approach. The top-down approach was used, as it is objective led, beginning with a general statement of the overall objective and expanding the initial values into more detailed concepts, which help to explain or clarify the former. A complete discussion of value trees, how they are constructed and used, can be found in Belton and Stewart (2002).

As a first classification of what to measure, it was decided to measure the three dimensions' knowledge (what you know), attitude (what you think) and behaviour (what you do). Each one of these dimensions was then subdivided into the six focus areas as discussed in Section 2 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*.

It is significant to note that the construction of the tree of aspects that could be measured is directly linked to the overall complexity of the model i.e. data gathering, importance weights for different factors, use and interpretation of results, justification for results, etc. Keeping it simple but meaningful was one of the major challenges in the design. An illustration of the tree structure developed is shown in Fig. 1.

Once the factors to be measured were identified, it was clear that they would not contribute in equal proportions to the final awareness level measurement. Therefore, another issue that needed to be measured was the importance of contributing factors. This was achieved through a measurement

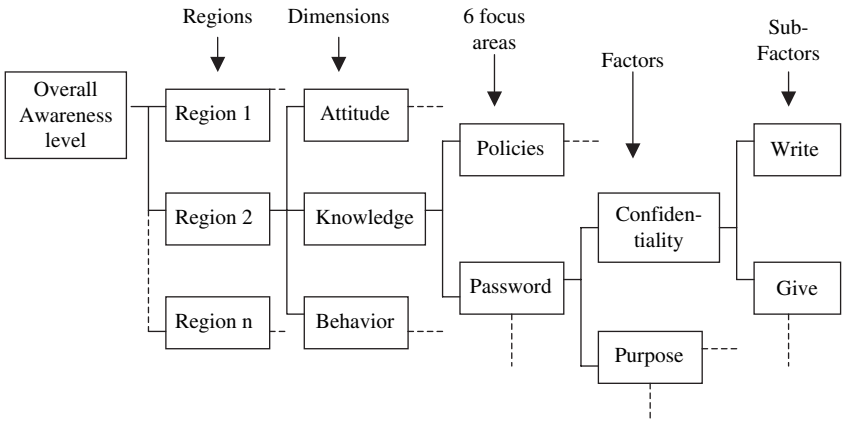


**Fig. 1 – Tree structure of problem.**

process where importance weights were allocated to all factors in a specific branch of the tree of factors. For example, the different regions will have different weights as they have different influences on the overall awareness levels; the three dimensions, knowledge, attitude and behaviour will have different importance levels; and the six focus areas will have different importance weights if management decides that it is more important to measure specific focus areas than others.

### 3.2. *How to measure*

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).

Scoring models are well known management science techniques and a complete description of the technique can be found in many textbooks. See for example Taylor (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 Delamater, 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 and Eloff (2001). Fig. 2 shows an example of a question in each of the three dimensions.

It is important to note that actual behaviour may not be measured accurately by a questionnaire alone as respondents do not necessarily tell the truth when asked about their behaviour. It should also be accepted that not all respondents will lie about their behaviour and that the use of a questionnaire will, in general, give at least an indication of the level of security behaviour. 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 incorporation of physical tests and other measures, to confirm actual security behaviour, forms part of an ongoing research process and is currently being investigated.

The importance weights, $w_i$, was determined using the analytic hierarchy process (AHP). The AHP approach makes use of pairwise 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. Saaty developed the AHP and a good description of the technical details and application possibilities can be found in Saaty (1980) and Vargas and Dougherty (1982). A comprehensive literature review of AHP applications in different fields and areas can also be found in Vaida and Kumar (2006).

The methodology outlined above complies with the organisation's specific requirements. It is *specific* to the mining company in the sense that it is based on the six focus areas as approved by senior management and it can be applied to each one of their regions to provide a final global awareness level. The method is *sustainable* as it can be applied over and over. It is fairly *easy* to use and output is given in a quantitative manner that is easy to understand. The techniques and principles used, such as value trees, scorecards and the analytic hierarchy process, are all accepted *scientific* methods that have been used numerous times before in research projects. In general the methodology provides a number of opportunities to benefit from.

- Not only will the model provide an overall global awareness level, but awareness levels are also measured (and reported

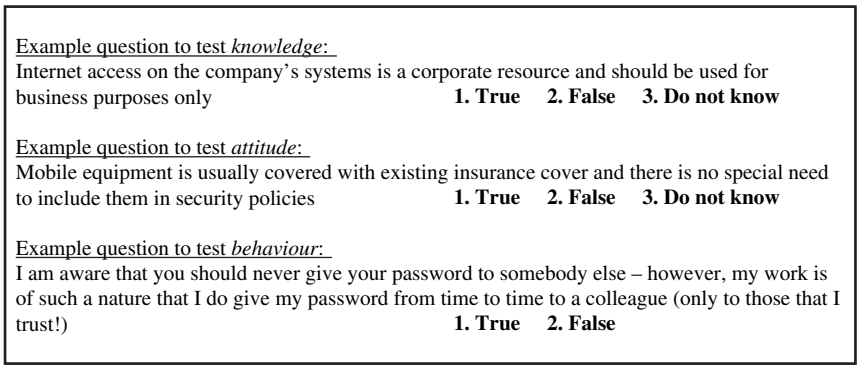


**Fig. 2 – Example questions.**

on) at intermediate levels i.e. per region, dimension, focus area and factor per focus area. If needed, low-level information from the questionnaires and importance weights can finally be used to explain specific performances.

- The data and the tree structure can be used to prepare a drill down system. Such a drill down facility would enable management to easily view the awareness at different levels of detail and plan accordingly what actions to take and where to focus these actions.
- By applying the model at regular intervals, the change in awareness levels can be measured and an index of awareness can be constructed. This will assist management to measure the change towards, or away from, security-positive behaviour over time, and to take corrective action if necessary. The index figure of awareness levels may also act as an important indicator of when to review, and possibly adjust, importance weights of those aspects being measured.
- Sensitivity analysis can be performed e.g. if management wants to change the importance weights of the different branches in the tree or when they want to study the effect of adding or deleting factors from the tree.

A possible negative aspect is the time it takes to perform the pairwise comparisons necessary to calculate the importance weights. This can take long depending on the number of factors identified in the tree structure as well as the number of managers involved in the process. Simplifying the process with user-friendly graphic interfaces or the use of an alternative weighting process is currently considered as part of the ongoing research process.

## 4. Application

The prototype tool was applied to the Australian regional office of the company discussed in Section 2. The choice of region was based on a management request as well as the fact that the environment (staff, infrastructure, etc.) was reasonably stable. The staff complement was small enough to easily obtain the required feedback and input, and all of them have already been exposed to the information security awareness program.

The first task was to determine what to measure. To this end, a value tree, similar to the one in Fig. 2, was constructed. From the tree, 44 aspects were identified that could be measured to cover the knowledge, attitude and behaviour dimensions with the associated six focus areas in each dimension. Next, a simple questionnaire, containing 35 questions (some questions were used to measure more than one aspect), to capture the information required was developed and tested at the region's head office as well as at one of the operational sites in the region. Different tests were performed and include tests using open-ended questions, multiple-choice questions, one-on-one contact with respondents and the use of e-mail facilities. These tests have provided valuable input and helped to refine the questionnaire. The refinement process took some time and involved a number of iterations with samples from staff to ensure that a model was developed which complies with the principles of sustainability, ease of use and scientifically sound. The final questionnaire was distributed and a response rate of almost 51% was recorded. Finally, the importance weights were determined using the AHP. The Information Security Manager, responsible for the organization's global information security, provided the pairwise comparisons to calculate the importance weights. Naturally importance weights will be based on input from all relevant managers – this study, however, was more focused on the feasibility and development of an acceptable methodology and therefore initial ratings from only one (and probably the most appropriate) manager were accepted as sufficient.

Questionnaire results and importance weights were processed in a spreadsheet application and output was finally presented in the form of graphs and awareness maps. Fig. 3 contains one example of a graph showing the overall awareness level (as being average) as measured with the prototype tool. Similar graphs were produced for each dimension as well as for each focus area. The following awareness scale, which was defined in accordance with management's view on awareness performance, was used to explain the level of awareness:

| Awareness | Measurement (%) |
|---|---|
| Good | 80–100 |
| Average | 60–79 |
| Poor | 59 and less |

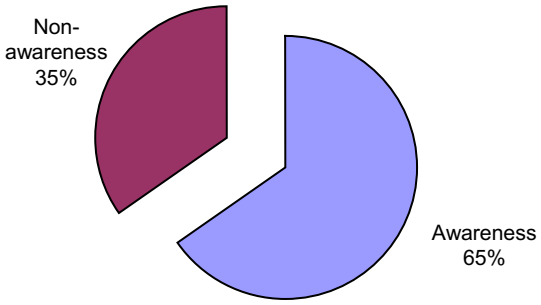


**Fig. 3 – Overall awareness level.**

The overall awareness in the region reviewed was measured as 65% and according to the awareness scale considered as 'average'.

The output of the measurement was also used to construct a colour coded 'Regional Awareness Map' – see Fig. 4(a). Using this map it is easy to see immediately how the region is performing in each dimension and each focus area. For example, Fig. 4(a) shows that the overall awareness for the region is 65%. This is made up by the three dimensions, which measured as 77% awareness in terms of knowledge, 76% awareness in terms of attitude, and 54% in terms of behaviour. The colour codes immediately show that information security behaviour in the region needs attention while knowledge and attitude were measured as average. The map also details measurements for each focus area. Consider for example the focus area *Adhere to policies* – the total awareness for this area is 44% and is made up of 18% awareness in terms of behaviour, 55% for attitude and 81% for knowledge. The colour codes suggest that the focus area needs attention and that the attention should be directed towards behaviour and attitude with acceptable knowledge. In the same manner, management can easily identify where to focus attention in each one of the six focus areas, thereby addressing the complete security awareness needs in the region.

Having produced a regional awareness map for each region, a final 'Global Awareness Map', consisting of the awareness levels in each region, can be constructed to show 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. Fig. 4(b) shows the global awareness map – the global awareness figure (86%) was inserted for illustrative purposes.

### 4.1. *Recommendations*

The prototype tool, as applied in practice, was in line with initial management requirements and was regarded as successful with significant results. This section will highlight some of the issues that were identified during the development and verification process that need more attention to ensure ongoing and effective use. The recommendations form part of an ongoing research and development process and some of them are currently being addressed.

- *A comprehensive and complete bank of questions should be developed*. It is recommended that some quality time be spent to research this aspect of the model more in depth. The model can only be successful if the ''right'' questions are asked to obtain correct data as input to the model. Cognizance should be taken from current best practices as described by various resources/organizations e.g. the Information Security Forum (ISF) and ISO 17799.

  A comprehensive set of questions is necessary to ensure, firstly that a different set of randomly selected questions is used every time the model is applied (if respondents have to answer the same questions every time, they might ''learn'' what the expected responses are) and secondly, to present different questions, randomly selected, to respondents in

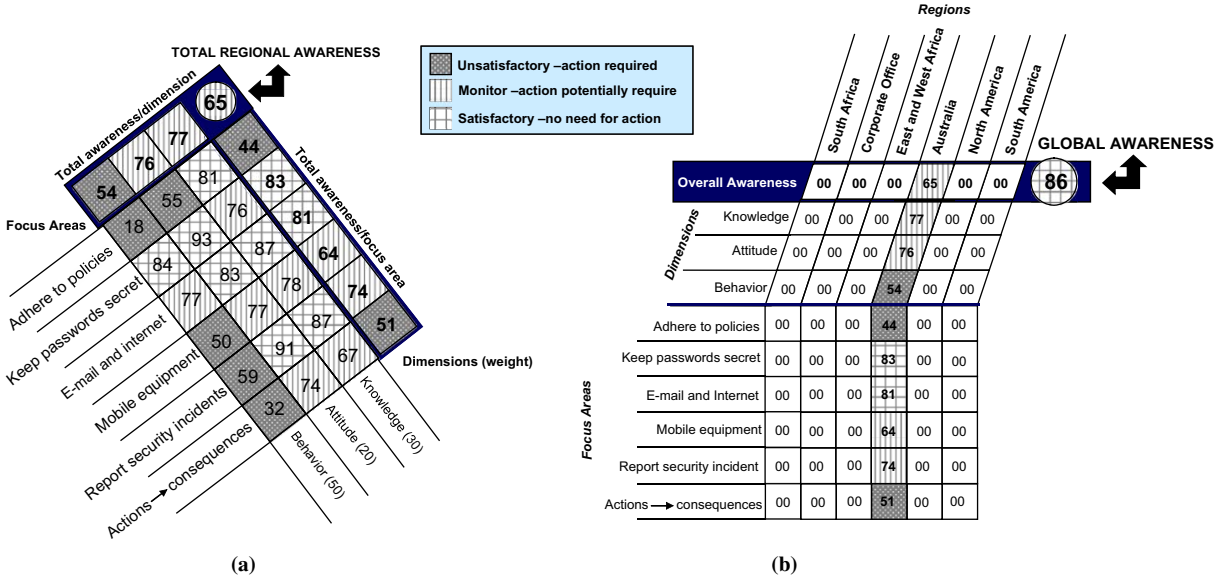


**Fig. 4 – (a) Regional awareness map of Australia; (b) global awareness map.**

the same office or region (to prevent respondents discussing questions and come up with consensus answers).

- *Importance weightings* should be obtained from relevant managers. The effectiveness of measurements, produced by the model, is dependent on proper evaluation (importance weights) of factors. These importance evaluations of factors are based on management's professional judgment and opinion and it is therefore imperative that the right level of management be identified and that sufficient time is allowed for gathering their ratings and then to convert it into input to the model.
- *The use of practical system data* obtained from, for example, a system administrator should be considered. Due to time constraints this was not fully explored during the test of the prototype. Practical data from a system could (should) be used as additional input to the model to test behaviour factors. Such data would be more reliable (not subjective or human dependent) and easy to get without making use of staff's working time to complete (longer) questionnaires. Examples may include number of virus infections, requests to visit unauthorized websites, number of IT security incidents, etc. To further enhance the quality of behaviour data, the Internal Audit department might be considered as an aid to assist with compliance tests.
- *The tool should be automated*. The information gathering process and the importance weight allocation process should be developed into a web-based tool that is controlled from a central point and then be made available to regions. The tool should:
  - Randomly generate a new set of questions every time it is used and then present it to the respondents
  - Facilitate the allocation of importance weights
  - Automatically feed the responses (questionnaires and importance weights) into the model
  - Solve the model and perform reporting activities (graphs, awareness maps and drill down facilities)
  - Keep track of responses from regions (database)
  - Keep track of awareness levels each time the model is applied
  - Automatically calculate, update and report on changes from one model application to the next (index figures)

## 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 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 offers several opportunities for enhancement and several 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. The tool will also be applied in other regions and more data will increase insight into the model and the framework and may lead to further enhancements.

## Acknowledgement

The authors would like to thank Prof Rossouw von Solms of the Nelson Mandela Metropolitan University for the useful comments and suggestions made. The authors alone are responsible for any errors and omissions.

## REFERENCES

Belton V, Stewart TJ. Multiple criteria decision analysis. An integrated approach. Dordrecht: Kluwer Academic Publishers; 2002.

CERT/CC. Date revised. CERT/CC statistics 1988–2004. Web: <http://www.cert.org/cert_stats.html>; 2004 [accessed September 2004].

CSI. CSI/FBI computer crime and security survey. Computer Security Institute; 2004.

Feldman RS. Understanding psychology. 5th ed. Boston, River Ridge, IL: McGraw-Hill College; 1999.

Furnell SM, Gennatou M, Dowland PS. A prototype tool for information security awareness and training. Logistics Information Management 2002;15(5/6):352–7.

Hansche S. Designing a security awareness program: Part 1, information. Systems Security January/February 2001:14–22.

ISF. Effective security awareness – workshop report. Information Security Forum; April 2002.
ISF. The standard of good practice for information security. Version 4.0. Information Security Forum; 2003.
ISO 17799. Information technology, code of practice for information security management. Geneva: International Standards Organisation; 2000.
Leach J. Improving user security behaviour. Computers and Security 2003;22(8):685–92.
Martins A, Eloff JHP. Measuring information security, <http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Martins.pdf>; 2001 [accessed August 2004].
Michener HA, Delamater JD. Social psychology. 3rd ed. Orlando, Florida: Harcourt Brace College Publishers; 1994.
Pentasafe. Security awareness index report: the state of security awareness among organisations worldwide. Pentasafe Security Technologies; 2002. p. 55.
Posthumus S, Von Solms R. A framework for the governance of information security. Computers and Security 2004;23(8):638–46.
Saaty TL. The analytic hierarchy process. McGraw-Hill; 1980.
Schlienger T, Teufel S. Information security culture – from analysis to change. South African Computer Journal 2003;31:46–52.
Spurling P. Promoting security awareness and commitment. Information Management and Computer Security 1995;3(2):20–6.
Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviours. Computers and Security 2005;24(2):124–33.
Taylor BW. Introduction to management science. 7th ed. Prentice Hall; 2002.
Teare G, Da Veiga A. Information security culture and awareness. Paper presented at the 2003 ISSA Conference, Sandton Convention Centre, South Africa; 9–11 July 2003.
Thompson ME, Von Solms R. Information security awareness: educating your users effectively. Information Management and Computer Security 1998;6(4):167–73.
Vaida OS, Kumar S. Analytic hierarchy process: an overview of applications. European Journal of Operational Research 2006;169(1):1–29.
Vargas LG, Dougherty JJ. The analytic hierarchy process and multicriterion decision making. American Journal of Mathematical and Management Sciences 1982;19(1):59–92.
Von Solms R, Von Solms B. From policies to culture. Computers and Security 2004;23(4):275–9.

**Kruger HA** is an Associate Professor in the School of Computer-, Statistical- and Mathematical Sciences at the North-West University (Potchefstroom Campus) in South Africa. He previously worked for Anglo American Corporation as a senior Computer Auditor and has more than 10 years experience in Information Risk Management. He has a PhD in Computer Science, a MCom (Information Systems) and an MSc (Mathematical Statistics). His current interests include decision modeling and the use of linear programming models.

**Kearney WD** currently works as a Manager, IT Risk and Compliance. He has over 15 years experience in Information Risk Management in a number of positions in large international companies, the last 5 years with AngloGold Ashanti. He has an MSc degree, numerous diplomas, and earned a number of certifications, including CISA and CIA. He was also successful in passing the CISM exam and has applied for certification. He is currently registered for a PhD (Information Security) and is a member of ISACA (Perth Chapter) and the Computer Society of South Africa.