International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:3, No:6, 2009

# A Prototype for Enhancing Information Security Awareness in Industry

E. Kritzinger, and E. Smith

***Abstract*****—**Human-related information security breaches within organizations are primarily caused by employees who have not been made aware of the importance of protecting the information they work with. Information security awareness is accordingly attracting more attention from industry, because stakeholders are held accountable for the information with which they work. The authors developed an Information Security Retrieval and Awareness model – entitled "ISRA" – that is tailored specifically towards enhancing information security awareness in industry amongst all users of information, to address shortcomings in existing information security awareness models. This paper is principally aimed at expounding a prototype for the ISRA model to highlight the advantages of utilizing the model. The prototype will focus on the non-technical, human-related information security issues in industry. The prototype will ensure that all stakeholders in an organization are part of an information security awareness process, and that these stakeholders are able to retrieve specific information related to information security issues relevant to their job category, preventing them from being overburdened with redundant information.

***Keywords*****—**Information security, information security awareness, information security awareness programs.

## I. Introduction

INFORMATION is the lifeline of many organizations and should therefore be properly secured and managed to ensure that it is not compromised in any way. If organizations fail to properly secure information, they could be faced with serious consequences, such as prosecution under a number of legal frameworks, or financial losses if information is compromised [1], [2]. There is thus a critical need to ensure that all users of information are made properly aware of how valuable information is, what the consequences are if they do not accurately secure the information they work with and what their role and responsibilities towards information security is [3], [4]. Based on the Global Information Security Survey conducted by Ernst & Young [2], among nearly 1,400 senior executives in more than 50 countries, people are still the weakest link in information security.

In spite of this realization a survey conducted by the Department for Business Enterprise & Regulatory Reform [5] shows that only 40% of the organizations participating in the survey provided ongoing security awareness training to staff. On the other hand, even if the best technologies are implemented to protect information within organizations, if the employees do not use these technologies properly, the information is still at risk [5]–[7]. Information security is therefore not only a technical issue, but also a human-related issue [1], [8]–[13]. In the industry sector, technical information security issues receive most of the attention when information security is addressed, and non-technical human-related information security issues are often ignored or neglected [14], [15].

When employees participate in an information security awareness exercise they are often overburdened with unnecessary information that is not relevant to their specific job function. It is unreasonable to expect that employees should be aware of *all* information security issues [16]. For example, an end user does not have to be aware of how to configure and maintain a firewall – this is the responsibility of the information security officers. Additionally, often the guidelines on how to secure information, focus on professionals in industry and leaves no room or opportunity for low-level users who require a scaled-down version of this knowledge [17], [18].

The authors accordingly developed an **I**nformation **S**ecurity **R**etrieval and **A**wareness model for industry – entitled "ISRA" [19]. The ISRA model will enhance information security awareness in the specific domain of industry, in the sense that it is based on a Common Body of Knowledge (CBK) for information security suited to industry, that draws a clear distinction between the *technical* and the *non-technical* information security issues. The ISRA model, however focuses on the *non-technical* information security issues only, to attend to the lack of attention that these issues currently receive as oppose to the technical information security issues. Additionally, the ISRA model does not only take the information security professionals into account, but incorporates *all* stakeholders in industry (including low-level users) that need to be aware of information security. The model ensures that stakeholders are made aware of the *relevant* information security issues that they need to be aware of in their job category only, preventing them from being overburdened with unnecessary information. Finally, the ISRA model incorporates a retrieval component, which will allow stakeholders to retrieve relevant information related to information security issues at any time. The information retrieved through this process can, for example, assist an Information Technology (IT) authority level (such as the Board level) in decision-making processes.

E. Kritzinger is with the School of Computing, University of South Africa, Pretoria, South Africa (e-mail: kritze@unisa.ac.za).

E. Smith is with the School of Computing, University of South Africa, Pretoria, South Africa (phone: +27-012-429-6309; fax: +27-012-429-6848; e-mail: smithe@unisa.ac.za).

The principal aim of this paper is to expound a prototype through which to implement the ISRA model. The prototype illustrates that the ISRA model is not merely a theoretical concept, but that it can indeed be implemented successfully. The prototype is used to achieve the main objective of the ISRA model, namely to enhance information security awareness among all employees. The first section of the paper will be devoted to an overview of the ISRA model as implemented by the prototype. In this way, a clear picture will be obtained of the purpose and deliverables of the prototype. The latter part of the paper will be devoted to an in-depth discussion of the prototype itself.

## II. Overview of the ISRA Model

The purpose of the ISRA model is not to discourage the use of existing information security awareness models, but rather to propose a new way of addressing and enhancing information security awareness.

### *A. Scope of the ISRA Model*

The scope of the ISRA model is first defined in terms of the information security community on which it focuses. The information security community primarily consists of the three main information security sectors namely *academia*, *government* and *industry* [20], [21]. Each sector should be aware of the specific information security issues (technical and non-technical) relevant to their sector. The ISRA model focuses specifically on the industry sector.

The scope of the ISRA model is also defined in terms of the CBK for information security. The ISRA model primarily focuses on the *non-technical* information security issues that are relevant to stakeholders in *industry*.

The aim of focusing on the non-technical information security issues is to counterbalance the traditional under-emphasis on non-technical information security research and implementations. It should be noted, however, that the technical information security issues are also important, but do not form part of the scope of the ISRA model.

### *B. Conceptual View of the ISRA Model*

The ISRA model consists of three parts namely, the ISRA Matrix, the Information Security Retrieval and Awareness part and the Measuring & Monitoring part – See Fig. 1.

#### *1. Part 1: ISRA Matrix*

The aim of the ISRA Matrix is to organize information regarding information security in such a way that retrieval of this information is fast and easy for all stakeholders. The ISRA model proposes a three-dimensional approach to enhance information security awareness in industry.

The three dimensions integrated to form the ISRA Matrix are information security documents, IT authority levels and non-technical information security issues – See Fig. 1.

These three dimensions can be represented as a cube – See Fig. 2.

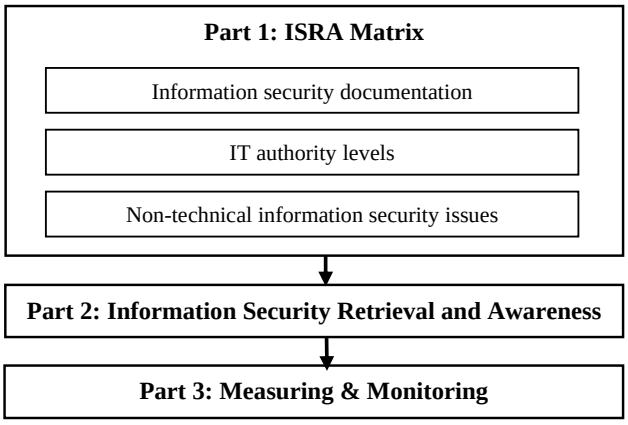


Fig. 1 A conceptual view of the ISRA Model

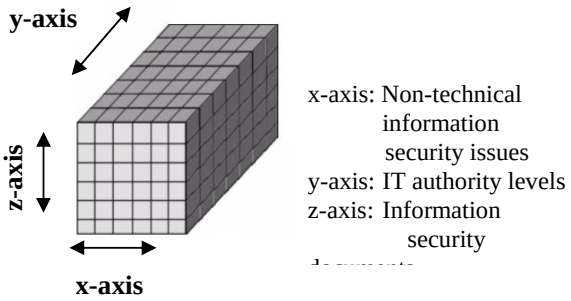


Fig. 2 Graphical view of the ISRA Matrix

The first dimension, consisting of leading national and internationally accepted information security documents, provides guidance with regard to information security issues. A vast amount of information security documentation is available today. For the purposes of the model ten of these documents that have an exceptional reputation and are widely known in the international information security environment, have been included. See Appendix A for a list of these documents. This dimension is depicted on the z-axis of the cube – See Fig. 2.

The second dimension includes the different IT authority levels (which consist of stakeholders) to which the content of the relevant information security issues should be transferred to. This will ensure that all stakeholders in the organization (not just the information security specialists) are exposed to all relevant non-technical information security issues. See Appendix B for a list of IT authority levels that form part of the model. This second dimension is represented on the y-axis of the cube – See Fig. 2.

Finally, the third dimension includes the different information security issues comprising the non-technical oriented part of the CBK of information security needed to secure information. See Appendix C for a list of the non-technical information security issues that form part of the model. This dimension is represented on the x-axis of the cube – See Fig. 2.

*2. Part 2: Information Security Retrieval and Awareness*

The second part of the ISRA model is the Information Security Retrieval and Awareness part. This part uses the ISRA Matrix to retrieve the relevant information requested by stakeholders. The advantage of the ISRA Matrix represented as a cube (See Fig. 2) is that the information within the cube can be viewed from different angles or viewpoints. For example, specific information regarding an information security document can be obtained by viewing the ISRA Matrix from the z-axis. The authors refer to this first retrieval method as the "z-slicing method". The z-slicing method extracts all relevant information regarding individual information security documents from the ISRA Matrix. Each z-slice will represent **one** document which includes the relevant information from the other two dimensions (IT authority levels and non-technical information security issues). Therefore, the z-slicing method will indicate which non-technical information security issues are important (relevant) and for which IT authority level, based on a specific information security document. This slicing method is depicted in Fig. 3.

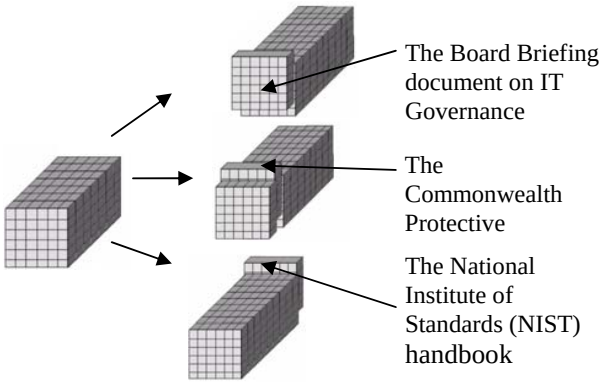


Fig. 3 Z-slicing

In the example depicted in Fig. 3 the first slice represents the information obtained from the Board Briefing document on IT Governance; the second slice represents information obtained for the Commonwealth Protective Security Manual and so forth. Similarly, the second retrieval method will view the information in the ISRA Matrix from the y- axis. The authors refer to this retrieval method as "y-slicing". The y-slicing method enables stakeholders to extract information regarding individual IT authority levels. Finally, the authors refer to the third retrieval method as the "combination-slicing method". This retrieval method is unique due to the fact that the slicing sequence within the ISRA Matrix will depend upon the request of the stakeholder. This retrieval method is used when more detailed information is required with regard to a specific IT authority level, non-technical information security issue and/or information security documents. The reader is referred to [19] to obtain more information on this retrieval method.

*3. Part 3: Measuring and Monitoring*

The last part of the ISRA model will primarily focus on the measuring and monitoring of the current information security awareness situation in an organization. Measuring and monitoring is a vital process in an organization and should be completed on regular intervals [7]. This will ensure that organizations know their information security awareness situation at any given time. This will also help the Board of Directors in their decision making process to ensure that if there is a security incident, it can be resolved before the availability, integrity and confidentiality of information is compromised.

## III. The Prototype

The prototype implements all three parts of the ISRA model. However, the combination-slicing method falls outside the scope of the prototype. The prototype was developed in a Windows 2003 environment using Visual Basic 6 and Javascript.

In a bid clearly to illustrate the functioning of the prototype, it is important to use the same example throughout the resultant discussion. The example chosen for this purpose is based on a small real-life optometrist institution in South Africa. This organisation comprises 3 IT authority levels i.e. Board of Directors level (consisting of the owner), Executive Management level (consisting of the partner) and user level (consisting of the secretary and the accountant).

### *A. Overview of the Various Sections of the Prototype*

When the prototype is loaded, it presents the user with a login screen where the user is required to enter a user-id and a matching password. After a successful login the screen depicted in Fig. 4 is displayed. This screen contains a menu bar with various menu options that enable a user to navigate through the program. The `Home` menu option should be selected to return to this screen at any time.

The `Edit` menu option enables the information security officer to populate the database with information regarding the body of knowledge, the information security documents, the employees in the organisation, the non-technical information security issues, the IT authority levels and the questions for an information security awareness program. The organisation under consideration outsourced their information security functions, and therefore do not have an information security officer.

The `Reports` menu option allows stakeholders (usually the Board of Directors and Executive Management level – unless access is granted to other stakeholders too) to extract statistical information from the database to examine the information security awareness status within the organisation.

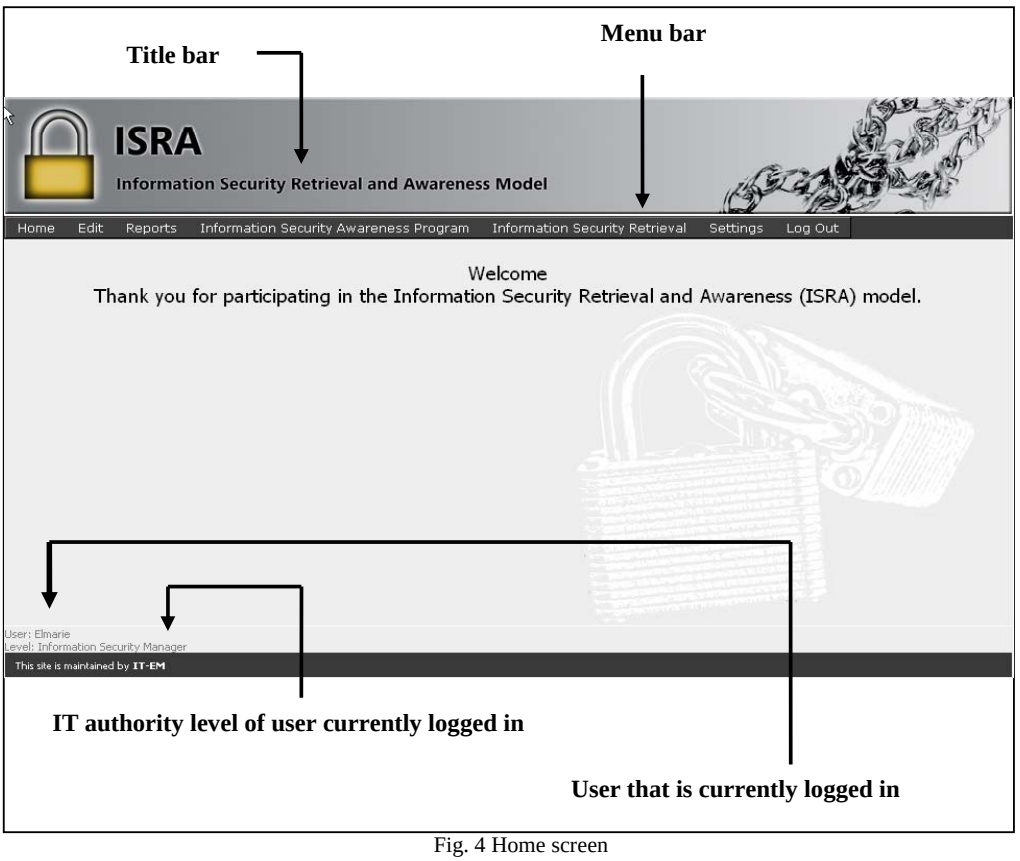


Fig. 4 Home screen

The `Information Security Awareness Program` menu option enables an employee to complete an information security awareness test on the information security issues related to the IT authority level of that employee currently logged in.

The `Information Security Retrieval` menu option enables an employee to retrieve information by either using the information security documentation as primary source and the information security issues as secondary source, or by using the information security issues as primary source and the information security documents as secondary source. The purpose of this option is to provide an employee with the information relevant to his/her IT authority level, with a view to improve the information security awareness of that employee.

The `Settings` menu option enables the owner to change the welcome message on the home page or to change the number of questions that form part of the information security awareness tests.

Finally, the `Log Out` menu option enables the user to log out.

*B. Functioning of the Prototype*

Following, a discussion on the real-life case in a bid more clearly to illustrate the functioning of the prototype.

Since all stakeholders in this organisation have access to sensitive information on a daily basis, they expressed a need for enhancing the information security awareness among all stakeholders in order to minimise the occurrence of human-related information security breaches. All stakeholders participated in the implementation phase of the prototype. They identified the following non-technical information security issues as currently being essential to their organisation:

- Computer ethics
- Physical security
- Corporate governance (including Information Security governance)
- Security policies

In addition, the owner required the following statistical information:

- The results of the information security awareness tests for each stakeholder.
- The information security risk areas in the organisation.

For the purposes of this paper, the discussion will be limited to the steps that the *owner* followed when he accessed the prototype (all the stakeholders used the prototype, but due to paper length the authors have not included all cases).

The first option selected by the owner was the Information Security Awareness Program option on the menu bar, and the screen that was displayed as a result is depicted in Fig. 5.

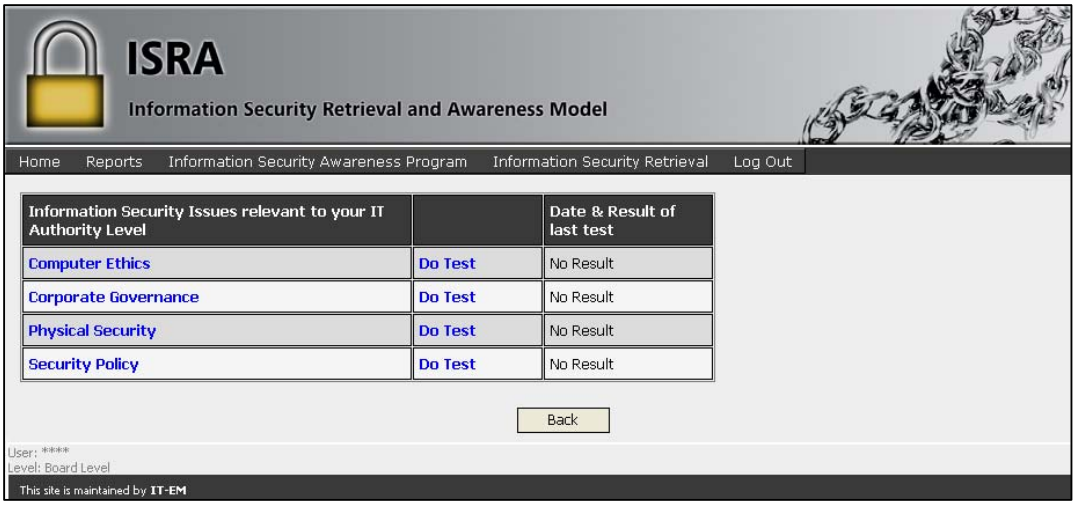


Fig. 5 Information Security Awareness Program screen

This screen lists all the non-technical information security issues relevant to the Board of Directors level (owner), with links to access information related to a specific information security issue (with a view towards preparing for a test). Additionally, links to complete an information security awareness test for each information issue are also provided. The screen furthermore displays the date and the result (0%-100%) of the last completed test – currently no tests have been completed by the owner. The four information security issues listed on the screen were indicated as important by the organisation. The prototype could easily be expanded if more issues become relevant.

The owner first viewed information on each of the non-technical information security issues listed by clicking on the appropriate links. Fig. 6 depicts the screen displayed when the owner clicked on the `Computer Ethics` link. A similar screen will be displayed for each issue.

Having read all the information displayed regarding the non-technical information security issues relevant to the Board of Directors level, the owner continued by completing one test for each non-technical information security issue by clicking the appropriate links. For the purpose of testing the prototype the authors constructed the necessary questions and answers for each information security awareness test. After each test had been completed, the initial screen (depicted in Fig. 5) was updated to reflect the results as depicted in Fig. 7.

The 'Date & Result of last test' column in Fig. 7 displays the result for each test, as well as the date on which each test was completed. Similar results will be available for all the stakeholders who completed the tests. These results are used in the reporting section to determine the information security awareness status of employees.

The second option selected by the owner was the `Reports` menu option. The owner wanted to determine the state of information security awareness among the **users**. The report displayed in Fig. 8 depicts the results (0%-100%) for each information security awareness test completed by the users (i.e. the secretary and the accountant). The username of the users were disguised to protect their identity. The latest test result that each user obtained in respect of a specific information security issue is displayed in tabular format. The user whose information is displayed in the first row, for example, obtained 56% for the information security awareness test on security policy, 75% for the information security awareness test on physical security and 44% for the information security awareness test on computer ethics.

In addition, a summary of the test results is displayed in graphical format (i.e. bar chart). The bar chart depicted in Fig. 8 displays the average test results regarding each information security issue. The average percentage (0%-100%) is depicted on the y-axis and the different information security issues are depicted on the x-axis. The average percentage of the two tests related to computer ethics – written by the secretary and the accountant respectively – is for example just above 40% (i.e. 41%). Based on this graphical representation, the owner concluded that the awareness of the users regarding *computer ethics* is poor and needs attention.

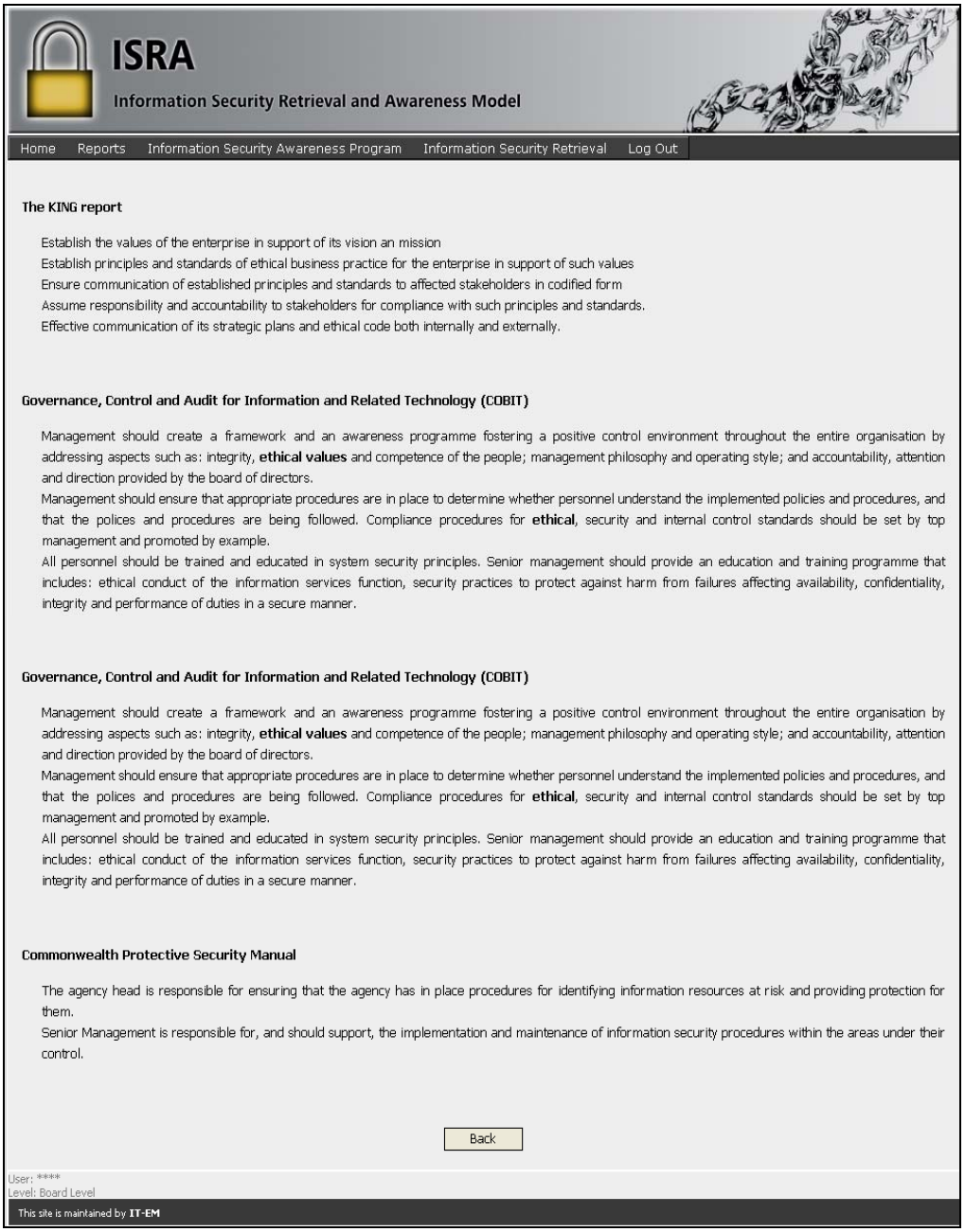


Fig. 6 Detailed information on computer ethics

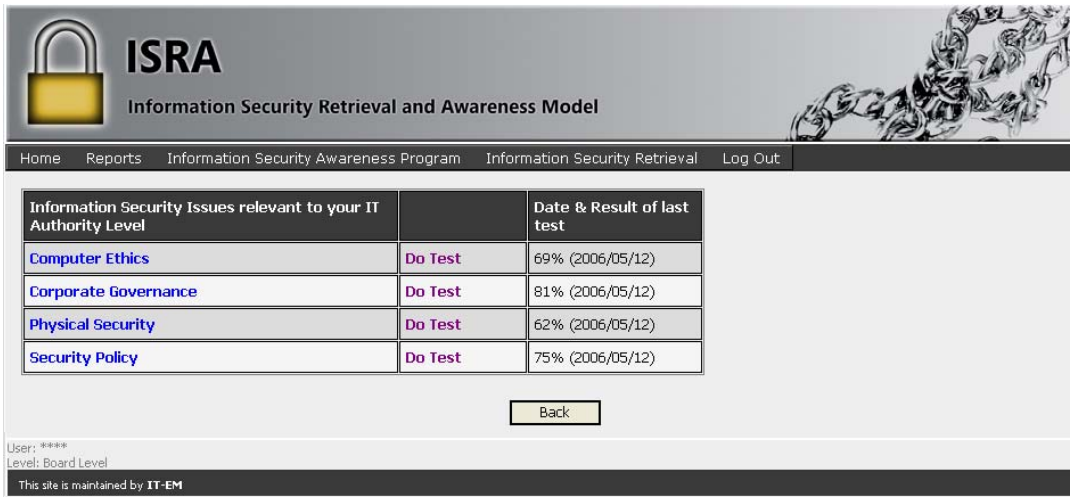


Fig. 7 Results for tests taken

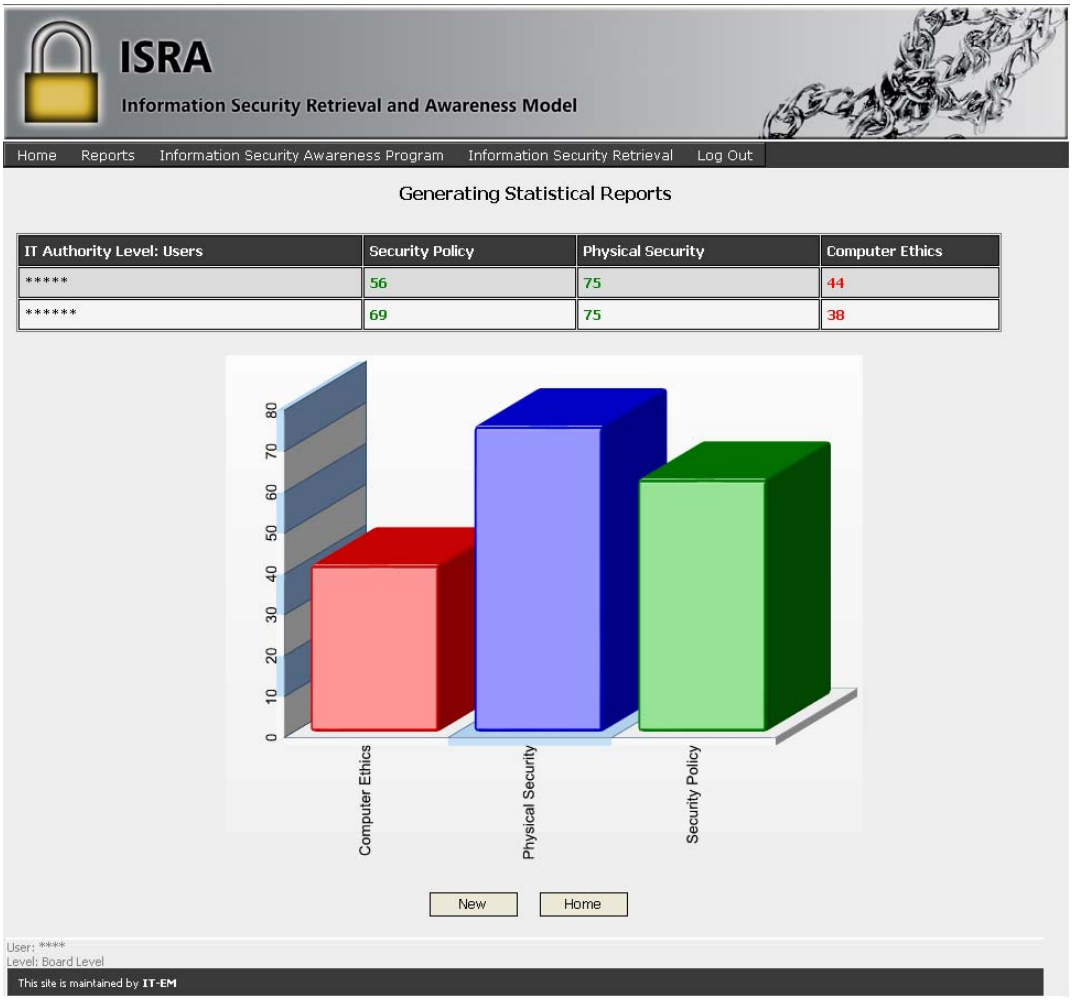


Fig. 8 Report requested


Fig. 9 Results of retrieval process

The last option selected by the owner was the `Information Security Retrieval` option on the menu bar. This option allows stakeholders to retrieve information directly from the database. It saves time and effort and no extra party needs to be involved. The owner decided to retrieve information regarding computer ethics on account of the low test results of the users in these issues (as depicted in Fig. 8). The screen depicted in Fig. 9 was displayed as a result.

## IV. Conclusion

This paper was devoted to expounding a prototype for enhancing information security awareness among employees within the industry sector. The prototype implemented all three parts of the ISRA model. The ISRA model is based on a CBK for information security specifically suited to industry. This CBK draws a clear distinction between technical information security issues and non-technical information security issues. The model as such focuses on the non-

technical, human-related information security issues. The ISRA model also ensures that *all* stakeholders in an organisation are part of the information security awareness process. This is achieved through assigning all stakeholders to a specific IT authority level. In addition, the ISRA model ensures that stakeholders are made aware of the non-technical, human-related information security issues related to their specific job category only, preventing them from being troubled with unnecessary information. Finally, the ISRA model incorporates a retrieval component, which will allow stakeholders to retrieve specific information related to information security issues at any time and without involving another party. The purpose of such a retrieval process is to enhance the information security awareness of the stakeholders.

The prototype is not meant to be a fully working system, but the purpose thereof is to enhance information security awareness among the stakeholders and to provide them with the opportunity to retrieve information directly from the database. The prototype illustrates that the ISRA model can be implemented successfully. The database used in the prototype can be populated to suit the specific needs of an organisation e.g. by adding IT authority levels as required. The reporting option enables top management to get a clear picture of the information security status of IT authority levels (and specific stakeholders) at a glance.

## Appendix A

**Information Security documents implemented by the ISRA model**

Board Briefing on IT Governance
Commonweatlh Protection Manual
Cadbury Report
COBIT
Information Security Governance
GMITS
ISO 17799
IT Infrastructure Library
King Report
NIST

## Appendix B

**IT authority levels implemented by the ISRA model**

Board level
Executive management level
Middle management level
Technical management level
Information security management level User level

## Appendix C

**Non-technical information security issues implemented by the prototype**

Physical security
Information security policies
Information security culture
Professionalism
Computer ethics
Legal issues
Corporate governance
Information security management
Risk management

## References

[1] Dlamini, M.T., Eloff, J.H. & Eloff, M.M., (2009). Information Security: The moving target. Computers & Security. Elsevier. Accepted 26 November 2008. Available online 11 December 2008. To be published.
[2] Ernst & Young, 2008. 2008 Global Information Security Survey: Moving beyond compliance. Available at: www.ey.com. Accessed on 17/02/2009.
[3] Dodge, R.C., Carver, C. & Ferguson, A.F., (2007). Phishing for user security awareness. Computers & Security. 26 (1): 73-80. Elsevier.
[4] Shaw, R.S., Chen, C.C., Harris, A.L. & Huang, H., (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education. 52 (2009): 92-100. Elsevier.
[5] BERR (2008). Department for business Enterprise & Regulatory Reform. 2008 Information Security Breaches Survey, Technical Report. PriceWaterhouseCoopers. Available at: www.berr.gov/sectors/infosec. Accessed on 17/02/2009.
[6] Morwood, G., (1998). Business continuity: awareness and training programmes, Information Management & Computer Security, 6(1): 28-32. Emerald.
[7] Von Solms, S.H., (2001). Information Security - A Multidimensional Discipline, Computers & Security, 20(6): 504-508. Elsevier.
[8] Peltier, T., (2005). Implementing an Information Security Awareness Program, Security Management Practices: 37-48. Available at: http://www.itknowledgebase.net/eJournals/articles/article_synopsis.asp ?id=89329. Accessed on 21/04/2006.
[9] Rostern, J., (2005). Dangerous Devices, The Internal Auditor, 62(5): 29-32. Institute of Internal Auditors.
[10] Theoharidou, M., Xidara, D. & Gritzalis, D., (2008). A CBK for Information Security and Critical Information Communication Infrastructure Protection. International Journal of Critical Infrastructure protection. 1 (2008): 81-96. Springer.
[11] Thomson, K. & Von Solms, R., (2005). Information Security obedience: a definition, Computers & Security, 24(1): 69-75. Elsevier.
[12] Von Solms, R. & Von Solms, S.H., (2004). The 10 deadly sins of information security management, Computers & Security, 23(5): 371-376. Elsevier.
[13] Waint, T.L., (2005). Information security policy's impact on reporting security incidents, Computers & Security, 24(6): 448-459. Elsevier.
[14] Ashenden, D., (2008). Information Security Management: A human challenge? Information Security Technical Report. 13 (2008): 195-201. Elsevier.
[15] Williams, P., (2008). In a 'trusting' environment, everyone is responsible for information security. Information Security Technical Report. 13 (2008): 207-215. Elsevier.
[16] Irvine, C.E., Chin, S.C. & Frincke, D., (1998). Integrating Security into Curriculum, Computer: 31(1212): 25-30. IEEE Computer Society.
[17] CSI/FBI (2005). Computer Crime and Security Survey, Available at: www.GoCSI.com. Accessed on 12/05/2006.
[18] Wilson, M. & Hash, J., (2005). Information Technology security awareness, training, education and certification, Available at: http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm. Accessed on: 12/04/2006
[19] Kritzinger, E. & Smith, E., (2008): Information security management: An information security retrieval and awareness model for industry. Computers & Security. 27 (5-6): 224-231. Elsevier.
[20] Crowley, E. (2003). Information Systems Security Curricula Development, in Proceedings of the 4th conference on IT curriculum on IT Education. p249-255. Lafayette.
[21] Hillburn, T.B., (1999). A Software Engineering Body of Knowledge Version 1.0. Technical Report, Software Engineering Institute.