Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.6, No.7, 2016
www.iiste.org

The Perceived Effectiveness of Information Security Awareness

Abigail N. W Prah[1] Angela Aba Otchere[2] Kojo Ennin Opan[3]
[1, 2, 3] Department of Computer Science, Takoradi Polytechnic, Box 256, Takoradi, Ghana.

Abstract
The need to protect information systems as much as possible from security threats and risks has risen in the last few decades due to the increase and sophistication of threats. The purpose of this dissertation is to examine the methods used to implement Information Security Awareness (ISA) programs. And also to investigate how the perceived effectiveness of ISA programs in preventing and mitigating security threats and risks organisations face, is assessed. The inductive research approach was used to explore the human side of the information security problem and how this impacts the perceived effectiveness of ISA programs. Then a prototype of a model to assess an ISA program was replicated. The results indicated that the awareness level of the region used for the implementation was average, meaning the ISA program was not as effective as it was expected to be. The model provides a guide to both researchers and practitioners in assessing ISA programs and obtaining statistical data or empirical data in order to prove how effective it is.

Keywords: Information Security Awareness, Information Security Policy, Information System, Security threats/risks and Perceived Effectiveness.

1. Introduction

The introduction of Information Technology (IT) has brought about the need for Information Security to keep the data produced safe from the various security threats and risks that affect the data. Information Security is defined by Whitman and Mattord (2010) as " the protection of information and its critical characteristics (confidentiality, integrity and availability), including the systems and hardware that use, store and transmit that information, through the application of policy, training and awareness programs, and technology". Information Security plays an important role in mitigating and preventing the impact of these security threats such as viruses, Trojan horses, phishing, spyware, etc. (Werlinger et al, 2009). There are various types of measure under Information Security and one of them is Information Security Awareness (ISA). Chen et al (2008, pg 361) state that "security awareness programs provide users adequate knowledge to evaluate adverse consequences of security problems and take the appropriate actions to prevent and correct security breaches". Thus ISA can be used by organisations to make their employees conscious of the security threats that could affect them and how this can be mitigated with security measures.

Amid the popularity of information security, security threats and risks keep rising, (ENISA, 2007a). Thus with all the advanced technical controls such as real time anti-viruses, high level physical security and firewalls that are implemented by organisations, there is still the increase of security breaches (Workman et al, 2008, pg 2805). This indicates that the technical side of the information security problem has been dealt with properly and it is left with the human side which is stated as being the weakest link in security (Zhang et al, 2009, pg 330 & Chen et al, 2008, pg 362). Even though people are the cause of most of the breaches, they are also the main way to detect, prevent and resolve the breaches or incidents, (Lacey, 2010, pg 4). ISA programs are used to handle this aspect in order to positively affect the behaviour and attitudes of employees towards information security. ISA programs involve every employee of an organisation and each organisation has its approach or method of implementing ISA programs. Some of the approaches used are interactive computer-based training, discussion sessions, online tutorials, training, and campaigns (Tsohou et al, 2008). The organisations that implement ISA programs gain some benefits from it. Some of the benefits are employees being able to recognize and respond appropriately to real and potential security threats, saving money by reducing the number of and extent of security threats, protecting customer and corporate information and improving compliance with organisations IS policies, standards and procedures (Native Intelligence, 2011).

Even though it is perceived that some well-developed ISA programs are effective in preventing and mitigating security risks and threats by implementing the programs with effective methods, the perceived effectiveness is not enough. Organisations will have to use methods to assess the programs that can provide some statistical or empirical data in order to prove its effectiveness.
The main purpose of this paper is to investigate how the perceived effectiveness of ISA programs in preventing and mitigating the impact of security threats in organisations is assessed. A lot is said about ISA programs, training and education and the stake holders know that it is very important and necessary (Tsohou et al, 2010). But less is said about how to assess its perceived effectiveness, (Kruger and Kearney, 2006, pg 290) and this

situation is the gap that has been identified, thus making the research that called for this paper necessary. Experts in ISA have different ways of assessing their programs but there is no one way to find out its perceived effectiveness. According to a research by ENISA (2007a, pg 2), every organisation has to find its right balance for their assessment because "there is no one size fits all".

To achieve the main objective, this paper intends to:

- Examine the methods or approaches used to implement ISA programs
- Examine how ISA programs are assessed
- Discuss the models and methods used currently to assess the perceived effectiveness of ISA programs.
- Build a practical application that will replicate a prototype of one of the models discussed.
- Inform managers, based on the prototype, on whether to improve, change completely or maintain their ISA program.
- To indicate the areas of the program that need immediate attention based on colour codes.

Does Information Security Awareness really mitigate and prevent the impact of security threats and risks in organisations? Investigating this question brings to focus how effective ISA programs are and this is the argument of this paper. It is thus imperative that we seek answers to the research questions below.

- What is Information Security Awareness (ISA)?
- What approaches or methods are used to implement ISA programs currently?
- What is the meaning of the perceived effectiveness?
- How are ISA programs assessed in order to determine its perceived effectiveness?

The significance of our paper could be linked to the fact that it will assist both researchers and practitioners in deciding which methods will be effective in implementing ISA programs for their specific security threats and risks they face. Also, it will help them in deciding which methods will be good for collecting the data needed to assess their program and then methods that will produce statistics in order to assess the ISA program. The statistics obtained will be used to obtain empirical evidence on whether their program is effective or not in mitigating and preventing security threats and risks. Thus they would not have to guess the effectiveness of their programs, the statistics will provide the empirical prove needed.

2. Methodology

In this section, we discuss the methodological considerations in this paper. The paper adopts the inductive research approach because of the human side or factor of the information security problem and how it relates to ISA programs. The human factor is seen as the first line of defence against security threats and risk. Thus to be able to understand how and why humans behave and act in certain circumstances in order to assess how effective an ISA program is, inductive research has to be used. Also, the case study method is used with the collection of secondary data. Primary data is not used because the data collected might be biased as no organisation would want outsiders to investigate if they are securely protected or not in relation to IT unless contracted by the organisation. The secondary data collected is reliable because it is from researches done over the years. Relevant literature in relation to ISA programs and its perceived effectiveness was selected from sources such as journals, books, dissertation and online articles. Then the methods of assessing ISA programs were examined, the effective ones were identified. Two case studies with prototypes for assessing the effectiveness of ISA programs in specific organisations will be discussed in the following section and one picked out to replicate. The replication will be discussed in the next chapter with its findings.

We discovered from the various literature that most organisations attempt to assess the knowledge, attitude and behaviour of their employees. This is done in order to determine if their ISA program has impacted any additional knowledge of security to their employees and if the program has been effective in preventing or mitigating the security threats. They attempt to use such methods as campaigns, computer based training, newsletters, emails, trinkets, brochures and flyers (Whitman and Mattord, 2008, pg 200) to assess the knowledge, attitudes and behaviours of their employees because if these three components are impacted positively, the impact of security threats and risks the organisations face will be mitigated and prevented. The choice of method depends on each organisation, their objective and target audience. Thus, based on this fact, a model was developed that demonstrates the components of an ISA program that is perceived effective as displayed in figure 1 below.

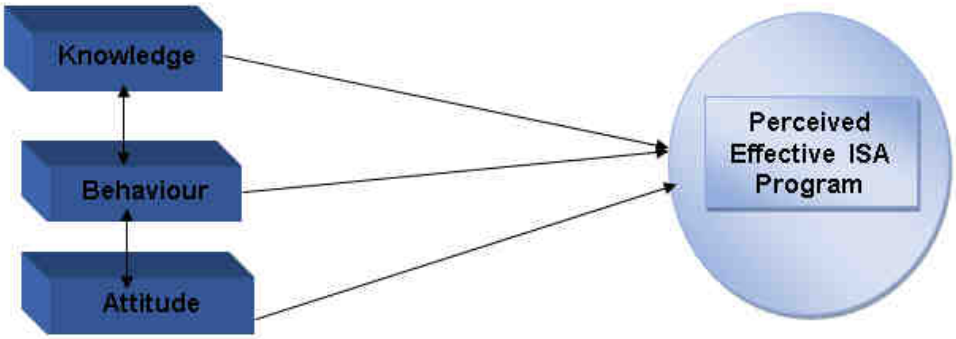

Figure 1: Components of a perceived effective ISA program

The three components, knowledge, attitude and behaviour are intangible characteristics of humans that most organisations attempt to assess in order to determine if their ISA programs are effective in mitigating and preventing security threats and risks. The organisations use some of the methods examined in chapter three to assess the knowledge, attitudes or behaviour of their employees. Others attempted to assess all three and based on the results of the assessment, perceived their program to be effective or not. Based on this model, it is presumed that if all the three components are assessed, then the results can be used to determine if a program can be called effective or not. This is because the knowledge of employees and their willingness to use the knowledge (attitude) they have will impact their behaviour. Thus, knowing the knowledge level of employees, their attitude towards security issues, how they react in certain situations and their willingness to use security procedures and controls all play a part in the impact of security threats and risks in an organisation. Also, if employees become more security conscious, the objectives of an ISA program are realised and security threats and risks are mitigated and prevented, then the program can be said to be effective. Therefore, the assessment of these three components can help an organisation to determine if they can call or perceive their ISA program as effective. As such, the two case studies were chosen based on what the organisations tried to assess.

2.1. Case Study One

Kritzinger and Smith (2009) developed the Information Security Retrieval and Awareness (ISRA) model and implemented a working prototype of it to enhance ISA in organisations and it focuses on the non-technical information security issues. The model is made of information such as security policies and procedures and it makes sure that only the relevant security issues are displayed to stakeholders. Thus only what is relevant to an employee's job is what they will be made aware of and they can also retrieve the necessary information needed on security issues at any time. The model consists of three parts as can be seen in figure 2 below.

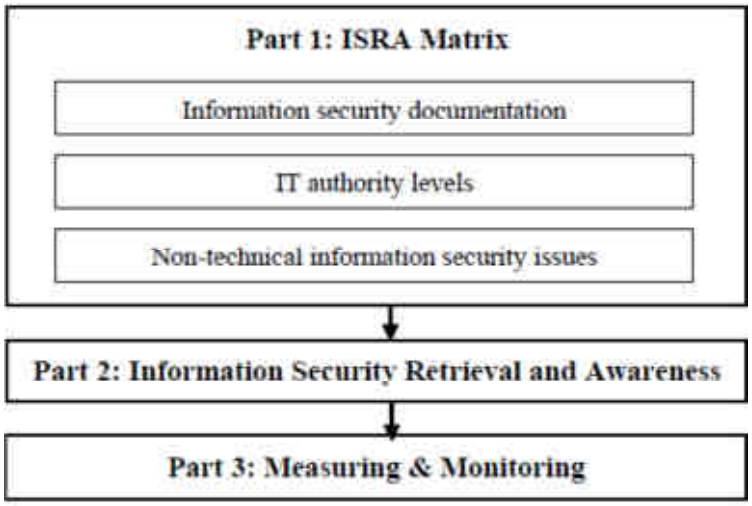

Figure 2: ISRA Model - Kritzinger and Smith, 2009, pg 1664

The first part of the model comprises of a collection of information security documents from various sources that is relevant to the organisation, the IT authority levels in the organisation and then the non-technical information security issues such as information security culture and physical security. The second part is the retrieval tool

that is used to retrieve the relevant information requested by the user. The third part is used to measure and monitor the ISA program and status of the organisation. It keeps records of security incidents reported before and after an ISA session and keeps records of results obtained after tests are taken by employees after an ISA program. The prototype was implemented for a small optometrist institution in South Africa. But this dissertation focuses on the third part of the model. The measuring and monitoring part comprises of a report menu that displays the ISA status of the organisation and results of test taken to stakeholders especially management, in statistical and graphical forms. Also, it has the ISA menu that allows an employee to take a test on any information security issue relevant to the IT authority level of the employee. Thus the employees of the optometrist could take tests on specific topics and see their results displayed and the management could see reports on all test taken and graphs on each topic. The company decided on the security issues that were relevant to them and wanted them in the prototype. Therefore tests taken were security issues that were relevant to the company and employees.

As such the prototype was tailored specifically to the company and its security issues. The questions developed for the test were questions that tested the knowledge of an employee, how they will react in a specific situation and how they perceive the security of the company. Here, it is identified that the three components described in figure 1 come up and the prototype uses its results from the test as a metric to determine the status of the ISA program in the company. This means that the status tells if the program is effective or not. The figures below are screen shots of the prototype.

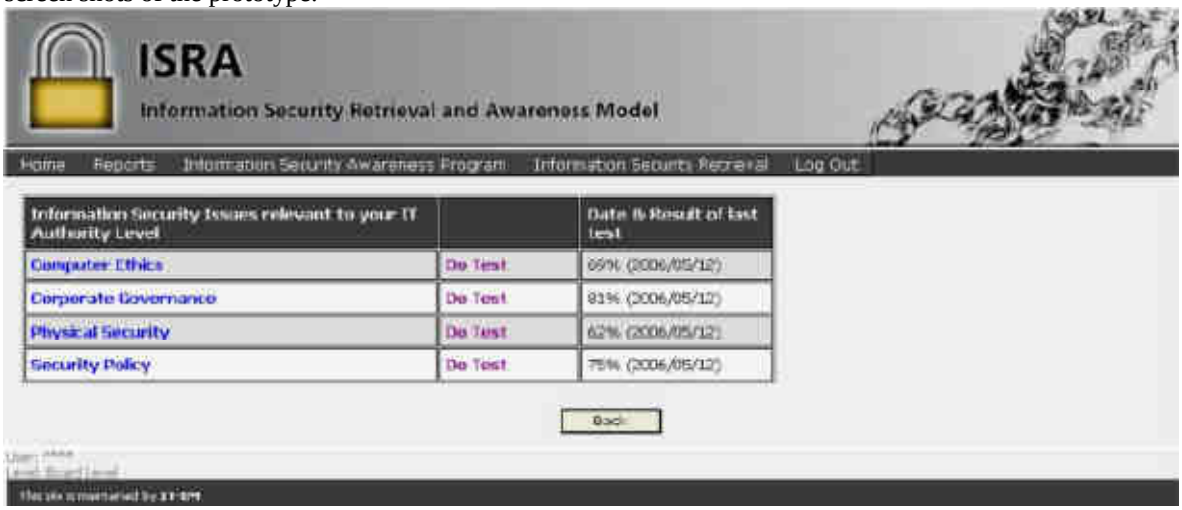

Figure 3: ISRA Prototype showing results for test taken - Kritzinger and Smith, 2009, pg 1669.

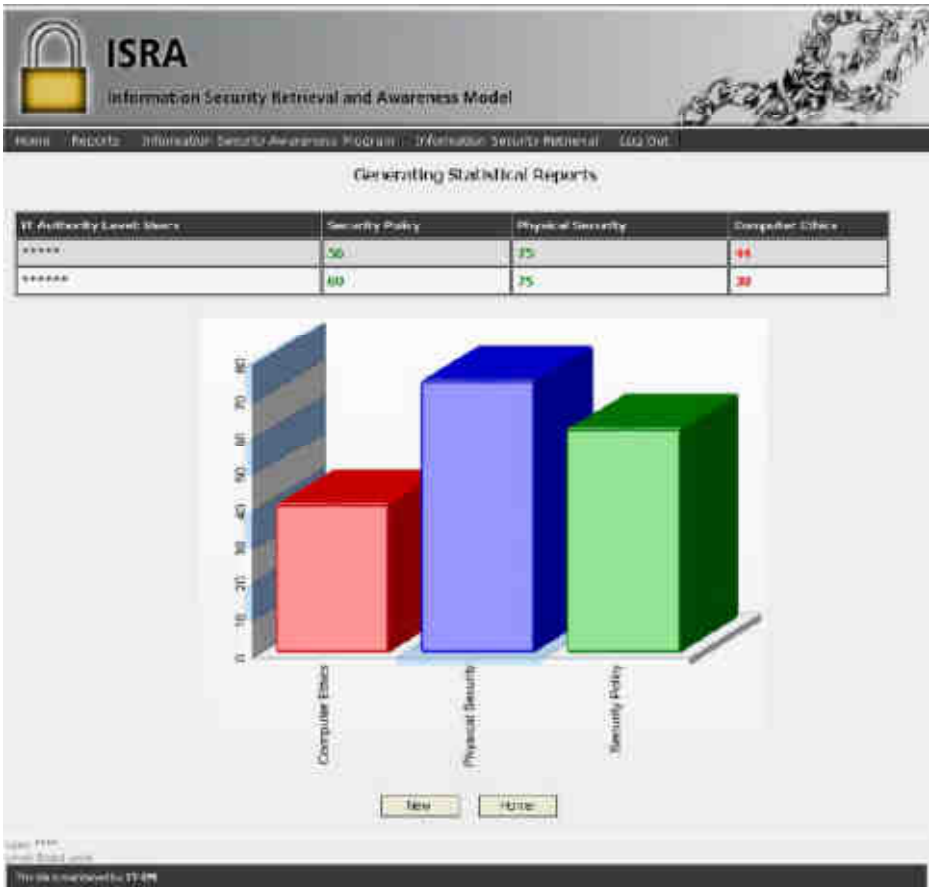

Figure 4: ISRA Prototype showing report requested for test taken - Kritzinger and Smith, 2009, pg 1669

2.2. Case Study Two

A model for assessing ISA programs was developed by Kruger and Kearney, (2006) and the prototype was implemented for AngloGold Ashanti which is an international gold mining company. The prototype was implemented after an ISA program specific to the security issues of the company was rolled out. The prototype was used to assess how effective the ISA program had been in meeting its objectives and what the current level of knowledge, attitude and behaviour of employees was, towards security issues of the company in relation to the ISA program they had gone through. A value tree was constructed that was used to determine the aspects of security issues that would be measured and that would cover knowledge, attitude and behaviour. A value tree is a simple representation that captures "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" (Kruger and Kearney, 2006, pg 291). The issues treated in the ISA program include adherence to policies, keeping passwords secret, email and internet, mobile equipment, reporting security incidents and actions – consequences. The security issues to be assessed based on the knowledge, attitude and behaviour of employees were decided upon by managers for all the regions of the global company. Since the relevance of the issues chosen is different depending on each region, the managers of each region decided on the weights of measure they should assign to each issue.
The prototype was implemented in the Australian regional office of the company. A questionnaire containing 35 questions was developed by the researchers. This covered open-ended questions and multiple choice questions and were used to assess an employee's knowledge, attitude and behaviour towards information security and the ISA program they had gone through. A sample of the questions and what they measure is shown in Figure 5 below.

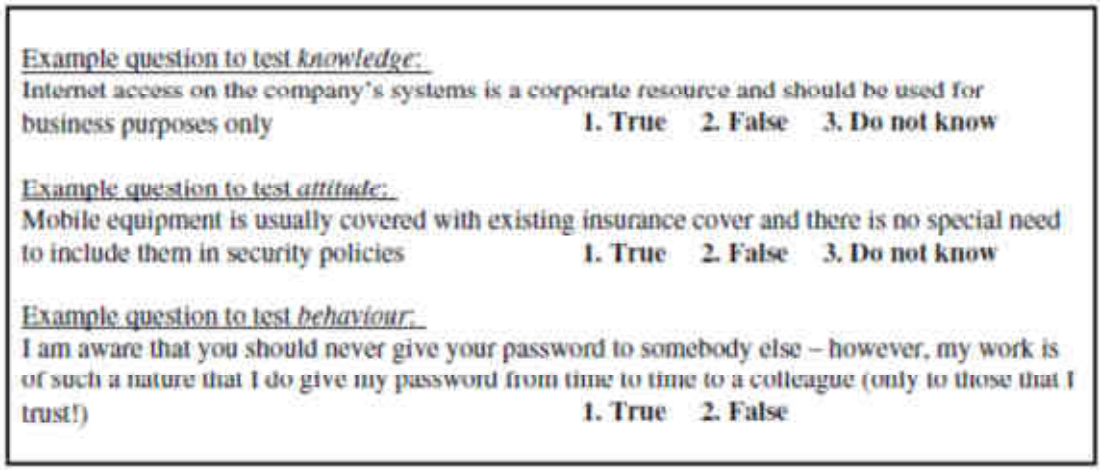

Figure 5: Sample of questions - Kruger and Kearney, 2006, pg 293

The importance weights assigned to each security issue relevant to the Australian region was determined using analytic hierarchy process (AHP). AHP is an approach that "makes use of pair wise comparisons to provide a subjective evaluation of factors based on management's professional judgement and opinion" (Kruger and Kearney, 2006, pg 292). After the approach, the weights assigned to the components were; knowledge – 30, attitude – 20, and behaviour – 50 for the Australian regional office. The results of the questionnaires and importance weights were then processed in a spreadsheet application and the output was presented in the form of graphs and awareness graphs. The awareness level of the region and the program's effectiveness was determined by a scale decided upon by the management. The scale used is seen in Table 1 below:

Awareness	Measurement (%)	Colour Codes
Good	80–100	Green
Average	60–79	Yellow
Poor	59 and less	Red

Table 1: Scale for awareness - Kruger and Kearney, 2006, pg 293

3. Results and Discussions

In this section, we discuss the results and findings of a prototype model. The issues assessed and their results will be discussed and what the results of this prototype means for the regional office of the international gold mining company. The limitations of this paper is also discussed.

The prototype of the model developed by Kruger and Kearney, (2006) was chosen for the practical aspect of this paper. This is replicated in a spreadsheet application. This prototype was chosen for the replication because it aligns or agrees with the model developed, named the components of a perceived effective ISA program. The prototype attempts to assess the components; knowledge, attitude and behaviour of employees. The three components combined, produce the perceived effectiveness of ISA programs. The issues treated in the ISA program are as follows; adherence to policies, keeping passwords secret, email and internet, mobile equipment, report security incidents and action-consequence.

Table 2: Regional awareness map of Australia

SERIAL NUMBER		COMPONENTS			TOTAL AWARENESS OF ISSUES
		Knowledge	Attitude	Behaviour	
	Weights of Components	**30**	**20**	**50**	
	Issues Addressed				
1	Adhere to policies	81	55	18	**44**
2	Keep passwords secret	76	93	84	**83**
3	E-mail & Internet	87	83	77	**81**
4	Mobile equipment	78	77	50	**64**
5	Report security incidents	87	91	59	**74**
6	Actions – consequences	67	74	32	**51**
	TOTAL AWARENESS OF COMPONENTS	**77**	**74**	**51**	67

The data for these six issues were collected by administering questionnaires to the employees of the Australian region. The questions were designed to assess employee's behaviour, attitude and knowledge; and weights were assigned to these components. The weights assigned to each component are as follows; knowledge – 30, attitude – 20 and behaviour – 50. The results of the questionnaires are in Table 2.
The data obtained from the questionnaires of the researchers were used for the replication of the prototype, (Kruger and Kearney, 2006, pg 294). The data was divided into the three components, knowledge, attitude and behaviour. From the data, the total awareness of the three components was obtained through the prototype. Data was obtained for each issue addressed in the ISA program. The employees were assessed through the questionnaires to determine what their knowledge, attitude and behaviour was in relation to the six issues addressed in the ISA program. The results for each issue are seen in Table 2. Out of the data, the total awareness of the components and issues were determined through the prototype. Also the total awareness of the region, 67, is determined through the prototype. Based on the scale used, as seen in Figure 12, 67 means the total awareness of the region is Average.

3.1. Findings/ Results

From Table 2, it can be seen that the behaviour of the employees towards the issues addressed in the ISA program is a bit on the downside. For instance with the issue 'Adhere to policies', the results indicate their behaviour to be 18. Based on the scale used, this figure means that the employees' behaviour towards the issue is poor. As such management will have to decide on how best to improve employees' behaviour in adhering to policies made. Also, the total awareness of behaviour in relation to the six issues addressed is 51, which is also poor based on the scale used. Thus, the behaviour of the employees mainly has to be checked by management. This is because if they have the knowledge, know what to do in a particular situation, know its importance but do not take any action, then the ISA program cannot be perceived as effective. Also since the three components together produce the perceived effectiveness, one component cannot account for the effectiveness. All the three components have to be combined to produce the perceived effectiveness.

Furthermore, the total awareness of each issue addressed in the ISA program is also determined in the prototype. With this, management will know which issues were disseminated effectively to employees and which issues were not, so that the methods of implementation can be changed or improved. For instance, the total awareness for the issue 'Keep passwords secret' is 83, which is good and is the highest number among the issues addressed. This means that the awareness for knowledge (76), attitude (93) and behaviour (84) of employees are all good and combine to produce the high awareness. Thus the method used to implement it was effective and it has reflected in the three components assessed. Management can therefore be assured that on this issue, problems would not arise frequently or it would be very low. Figure 6 below shows a graph of the six issues and their percentages obtained for each component.

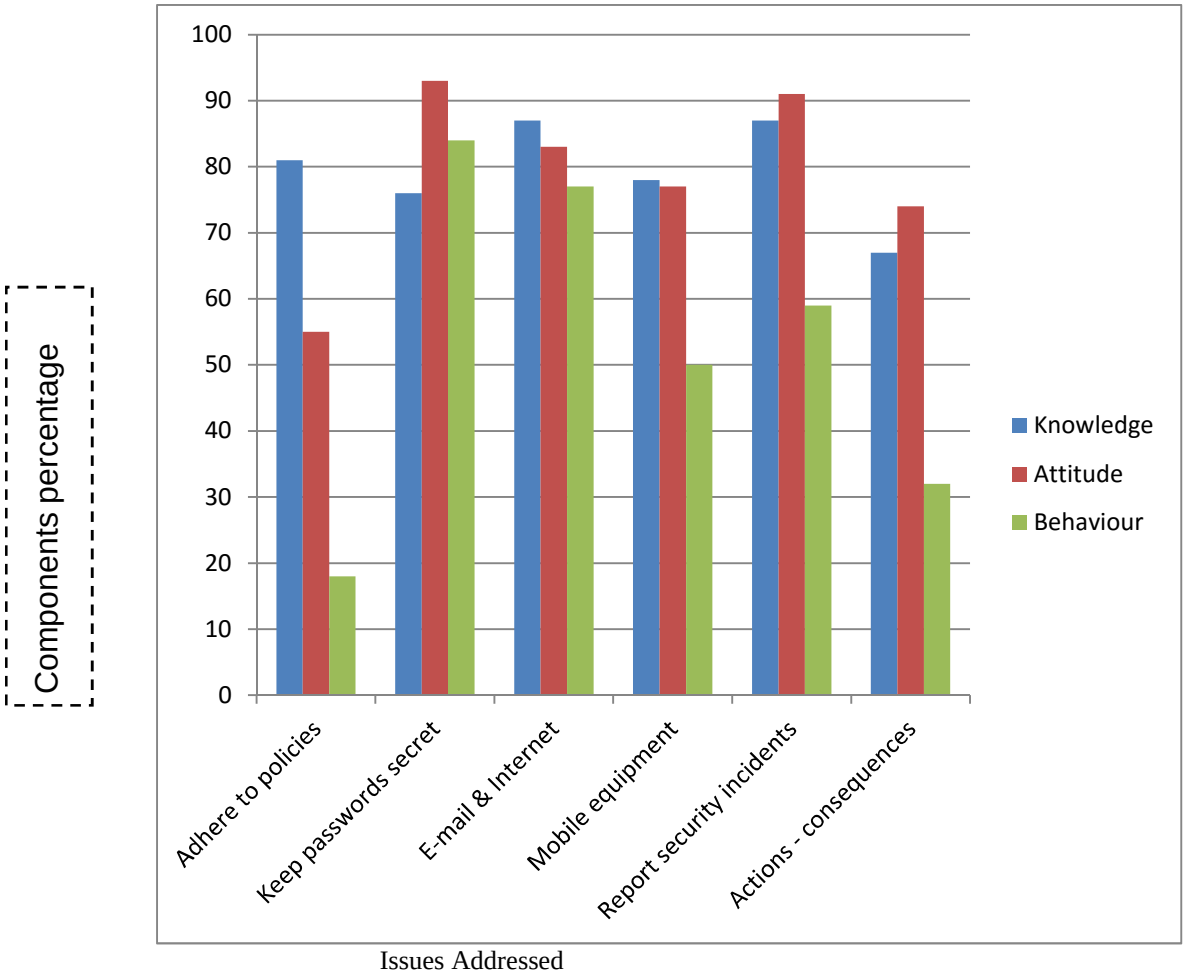

Figure 6: Graph of issues and components (a)

Figure 6 indicates the percentages of the three components in relation to the six issues addressed in the ISA program. The differences in the knowledge, attitude and behaviour of the employees of the Australian region can be seen in relation to the issues. For the issue 'Report security incidents', knowledge is 87, attitude is 91 and behaviour is 59. This indicates that the behaviour towards the issue is average and it has to be improved in order for it to be good.

Figure 7 also represents a line for the percentages for each of the three components to be clearer. The graph below shows how each component rises and falls in relation to each issue. From this, it can be seen that the behaviour of employees is generally low whilst their knowledge and attitude is a bit high.

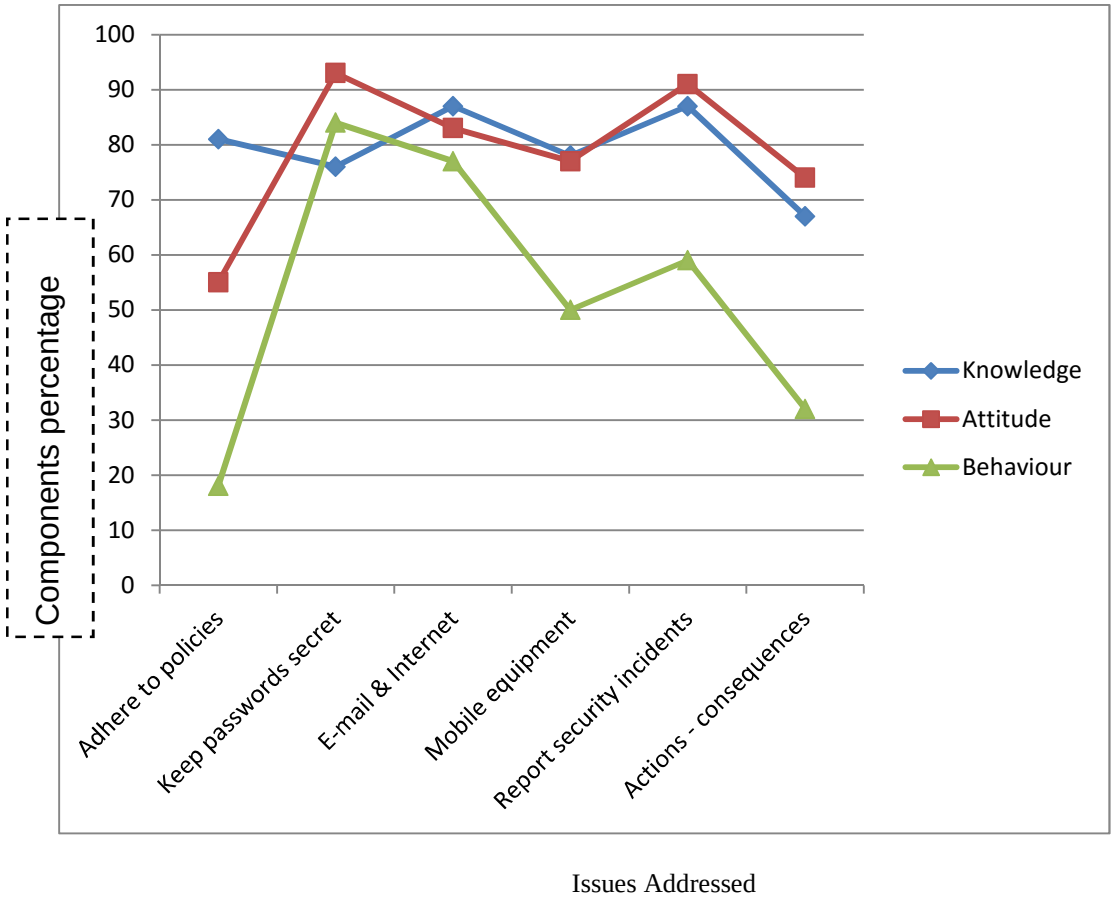

Figure 7: Graph of issues and components (b)

Also, the figure of each component in the region is determined through the prototype. The total knowledge awareness of the region in relation to the issues addressed in the program is 77% which based on the scale used is good. This means that the employees had obtained enough knowledge on the issues addressed on the ISA program. The total attitude awareness of the region in relation to the issues addressed is 74% which is also good based on the scale used. Also, the total behaviour awareness of the region in relation to the issues addressed is 51% which is poor and as stated earlier should be checked and improved in order to achieve the perceived effectiveness of the ISA program. Figure 8 is a graph of the total awareness of each component and it indicates the level of awareness of each component.

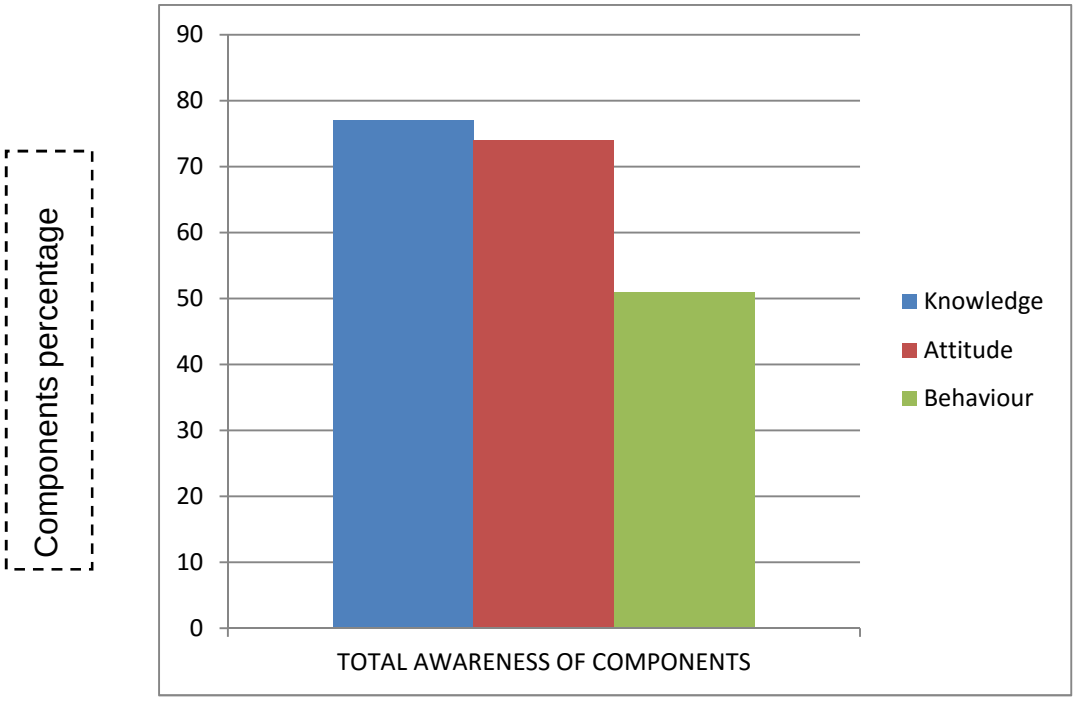

Figure 8: Graph of total awareness of each component

3.2 Discussion

The results in Figure 8 above indicate that the behaviour of the employees of the region has to be improved in relation to information security. Even though the total awareness of the region is 67, thus average, it is good that the awareness of each component assessed is also provided. With the awareness of each component, management will know which specific area to tackle in order to improve it. The results in figure 16 indicate that the total awareness of the behaviour of employees which is 51 is below average or it is poor. This means that even though they know how important the issues addressed in the ISA program are, they do not care enough about using the knowledge they have gained in protecting the information system of the company. As such management can use this information to investigate why the employees are not behaving as expected in issues concerning security. When that is figured out, they can then rectify the situation, then employees' behaviour will improve and they will use the technical controls and procedures provided to keep the company secured.

Also, the total awareness of knowledge of the employees is 77 is good (see Figure 8). This means that the employees had gained enough knowledge in the issues addressed on the ISA program and also that the methods used to implement the ISA program on the whole were effective. Therefore management can use the methods for a while and then change it so the employees do not get too used to it. But taking a look at the result for the total awareness for behaviour, it can be stated that, the fact that employees have the knowledge does not necessarily mean that they will use it. The methods used to implement the program were effective and the message got across clearly but that did not affect their behaviour. As such how effective an ISA program is cannot be based on just one of the components. In reference to the model developed in chapter four, the components of a perceived effective ISA program, the three components have to be combined to produce the perceived effectiveness. Therefore, if only the knowledge of the employees was assessed, then management can conclude that the program was effective and this would have been a wrong perception because it does not reflect in their behaviour.

Furthermore, the result of the total attitude awareness of the employees is 74, as Figure 8 illustrates, and it is also good based on the scale used. This means that the employees see the importance of the issues addressed in the program and are willing to act on the knowledge gained. But from the results of the total behaviour, it seems they are not motivated enough to put their knowledge and attitude in action. This indicates that the management have no problem with the knowledge and attitude of the employees; just their behaviour and they have to investigate what the problem is in order to resolve it.
It imperative that the result for each component in relation to the issues addressed be checked by management so

they know which area to make changes or just improve. The colour codes in Table 2 will help the management identify quickly which areas need attention and they can work on it. The areas coloured red, meaning poor will need immediate attention if management wants to have an effective program and the preventing and mitigation of security threats and risks.

4. Conclusion and Recommendations

An important reiteration, based on our results, is the fact that perceiving the program to be effective based on just one component will not be a good idea. As noted in the literature, most authors (Davis 2008, Kruger and Kearney 2006, Lacey 2010, Styles and Tryfonas 2009, ENISA 2007) agree that the knowledge, attitude and behaviour of employees combine to produce an effective ISA program which in turn will help in preventing and mitigating security threats and risks organisations face. As such the three components are essential in determining if a program is effective or not because they all constitute integral aspects of human characteristics. Therefore, for an organisation to meet its objectives or goals set for an ISA program, these three components have to be impacted positively. Though it is difficult to measure these components, organisations and researchers attempt to do so with the methods discussed and then analyse the results statistically. This is how the prototype was operated in order to provide the results obtained.

It is our respectful recommendation that more models are developed by both practitioners and researchers that provide statistical data in order to have empirical evidence of how effective ISA programs are. This call, in our view, will assist in reducing the constraints likely to be posed by insufficient models that can attempt to assess the effectiveness of an ISA program. Eventually, the effectiveness of ISA programs can be proven and not be perceived anymore. Also, the prototype replicated in this paper is a spreadsheet application. Further we suggest a research into the development of a sophisticated software that will make the work of management in assessing easier. Additionally, other methods apart from questionnaires can be used to collect data. This will give a more complete picture of the state of awareness in an organisation. The questions used in any of the methods chosen should be changed frequently so that employees do not give already known answers.

References

Chen, C. C. & Medlin, D. B. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*. 16(4): 360-376.

Choi, N., Kim, D., Goo, J. & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security*. 16 (5): 484-501.

D'Arcy, J., Hovav, A. and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*. 20 (1): 79–98.

Davis, P. (2008). Measuring the effectiveness of information security awareness training. SAI Global, Retrieved from www.saiglobal.com/.../how-to-measure-information-security-training .

Great Britain. The Department for Business, Innovation and Skills (BIS), (2010). Information Security Breaches Survey (ISBS) Technical Report. London. Retrieved from http://www.infosec.co.uk/files/.

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*. 25(4): 289-296.

Kritzinger, E. & Smith, E. (2009). A prototype for enhancing information security awareness in industry. *World Academy of Science, Engineering and Technology*. 54: I663-1671.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*. 18 (1): 4-13.

Native Intelligence, Inc. (2011). Information Security Awareness and Privacy Training Programs. Retrieved from http://www.nativeintelligence.com/ni-programs/ni-benefits.asp .

Stewart, G. B. (2009). Maximising the effectiveness of information security awareness using marketing and psychology principles. Master's Thesis. Royal Holloway, University of London. Retrieved from http://www.media.techtarget.com/searchSecurityUK/.../RHUL_Stewart.

Styles, M. & Tryfonas, T. (2009). Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users. *Information Management & Computer Security*. 17 (1): 44-52.

The European Network and Information Security Agency (ENISA), PricewaterhouseCoopers. (2007a). Information Security Awareness Initiatives: Current Practice and the Measurement of Success. Retrieved from www.enisa.europa.eu/act/ar/deliverables/2007/.

The European Network and Information Security Agency (ENISA). (2007b). Information security awareness: local government and internet service providers. Retrieved from www.enisa.europa.eu/act/ar/deliverables/2007/.

Tsohou, A. et al. (2008). Investigating information security awareness: research and practice gaps. *Information*

Security Journal. 17 (5/6): 207-227.

Tsohou, A. et al. (2010). A security standards framework to facilitate best practices awareness and conformity. *Information Management & Computer Security.* 18(5): 350-365.

Werlinger, R., Hawkey, K. & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security.* 17(1): 4-19.

Whitman, M. E. & Mattord, H. J. (2008). *Management of information security*. *3rd Ed*. Course Technology, Cengage Learning.

Whitman, M. E. & Mattord, H. J. (2010). *Management of information security*. *3rd Ed*. Course Technology, Cengage Learning.

Workman, M., Bommer, H. W. & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behaviour*. 24(6): 2799-2816.

Zhang, J., Reithel, B. J. & Li, H. (2009). Impact of perceived technical protection on security behaviours. *Information Management & Computer Security.* 17(4): 330-340.

ISA posters. (2011). Retrieved from <http://www.infosecuritylab.com/index.php?page=9.