An assessment of the role of cultural factors in information security awareness

HA Kruger
School of Computer Statistical and Mathematical Sciences
North-West University
Potchefstroom, South Africa
Hennie.Kruger@nwu.ac.za

S Flowerday
Information Systems
University of Fort Hare
East London, South Africa
Sflowerday@ufh.ac.za

L Drevin
School of Computer Statistical and Mathematical Sciences
North-West University
Potchefstroom, South Africa
Lynette.Drevin@nwu.ac.za

T Steyn
School of Computer Statistical and Mathematical Sciences
North-West University
Potchefstroom, South Africa
Tjaart.Steyn@nwu.ac.za

Abstract— **An information security awareness program is regarded as an important instrument in the protection of information assets. In this study, the traditional approach to an information security awareness program is extended to include possible cultural factors relating to people from diverse backgrounds. The human factor, consisting of two closely related dimensions, namely knowledge and behaviour, play a significant role in the field of ICT security. In addition, cultural factors also impact on the security knowledge and behaviour of people as cultural differences may manifest themselves in different levels of security awareness. An information security vocabulary test was used to assess the level of awareness pertaining to the two human dimensions – knowledge and behaviour amongst students from two different regional universities in South Africa. The objective is to determine whether cultural differences among students have an effect on their ICT security awareness levels. Results obtained suggest that certain cultural factors such as mother tongue, area where you grew up, etc., do have an impact on security awareness levels and should be taken into consideration when planning and developing an information security awareness program.**

Keywords - ICT security awareness; cultural factors; vocabulary test

I. INTRODUCTION

The protection of information assets usually relies on the success of information security plans and the implementation of various security controls as part of such a plan. Apart from the usual technical controls, there is also considerable dependence on human involvement and this human factor in information security is directly related to human behaviour and knowledge. This means that humans involved in a security process need to possess the required knowledge about their security related roles, and thus need some form of education [1]. Schneier's [2] findings in this area are significant as they highlight the importance of this issue; his study concludes that 62% of employees have limited information security knowledge and this exacerbates the ICT awareness problem.

Therefore, in this paper the traditional approach to an information security awareness program is extended to include possible cultural factors relating to people from diverse backgrounds. The human factor, consisting of two closely related dimensions namely knowledge and behaviour play a significant role in the field of ICT security. Accordingly, culture refers to the beliefs, values and assumptions that a group has learnt over time [3]. Thus, this paper investigates if cultural factors impact on the security knowledge and behaviour of people as cultural differences may manifest themselves in different levels of security awareness.

The remainder of this paper is organised as follows. In section II a brief theoretical background is provided followed by the methodology presented in section III. Section IV discusses the results of the empirical test and section V concludes the paper with some final comments.

II. THEORETICAL BACKGROUND

Dhillon [4] proposes the notion that informal behaviour is fundamental in describing those characteristics of people, organisations, and acts of communication which together affect information. This notion purports that the management of information security connotes the management of integrity of communications. Indeed the argument continues that communication and behaviour should be considered as opposite sides of the same coin. Therefore, "any discordance in the behavioural patterns could potentially lead to security problems". This lends itself to the understanding that there is a cause and effect relationship between unwarranted behaviour, breakdown in communication, and a possible security breach. This idea of considering information systems and communication as one and the same thing is not new. The concept considers processes of communication as the central hub of information systems. Indeed, Dhillon states

"information systems facilitate communication, and the organisations are woven from threads of communication". Hence any problem with the system of communication directly affects the information system that facilitates it and vice-versa [4].

This adds to the position where anthropologists and sociologists have traditionally considered such interactions as being essential to generate human learning. Furthermore, interactions and learning are grounded in the prevalent culture [4]. Additionally, it is said that patterns of learning, culture, and existing norm structures are all constituent elements of informal behaviour. Thus, one can reasonably conclude that complete management of information security can be ensured only if the behavioural aspects of individuals and groups are understood.

This line of reasoning emphasises the importance of this paper which seeks to establish if cultural differences among university students have an effect on their ICT security awareness levels. This paper is building on the work of a previous study which performed an information security vocabulary test in order to draw conclusions about a group's information security awareness levels [5]. The motivation for these studies is that if a person does not have a basic comprehension of ICT security terms and concepts, then one is probably more susceptible to becoming a victim of cybercrime. The theoretical justification for using a vocabulary test is described in [5].

Briefly, the vocabulary test is based on three key cognitive skills that are necessary to ensure a successful learning experience. They are [6]

- Knowledge of facts, processes and concepts;
- The ability to apply the knowledge, concepts and processes; and
- The ability to reason.

A summarized explanation of the three required cognitive skills as they pertain to information security awareness is given below in table 1.

TABLE 1: COGNITIVE SKILLS (ADAPTED FROM [7])

Cognitive category	**Cognitive action**	**Explanation**
Knowledge of facts, processes, procedures and concepts (what someone needs to know)	Recall, recognize, calculate, derive information from graphs or tables, measure, classify, sort	When people do not have reasonable access to a knowledge- or facts-base in information security, focused information security reasoning becomes difficult. Knowledge of security processes (steps, methods or procedures) forms the link between basic knowledge and the implementation thereof. Knowledge of information security concepts enables people to see the relationship among the different elements of information security and helps to ensure that facts are not seen or treated in isolation.
Understanding and application of knowledge	Choose, suggest, develop a model, solve problems and implement solutions	Representation of information security ideas forms the basis of perceptions and communication in information security and is a basic prerequisite for a successful information security environment. When it is expected from someone to apply knowledge in the information security area, the type of problem should be known in order to execute the required procedures and to choose the best strategy for solving the problem.
Reasoning (focus on solving problems in unknown situations)	Analyze, generalize, integrate, defend solutions	Reasoning in information security requires a logical and systematic approach which would include intuitive and inductive thinking processes. People should be able to implement expertise in different contexts.

With this brief introduction and theoretical background in mind it was decided to use a vocabulary test, in conjunction with certain cultural information as basis of a new measuring instrument for this study, to assess the ICT security awareness levels of students and to determine whether cultural factors play a role.

III. METHODOLOGY

As explained in section II, a security awareness questionnaire, based on a respondent's vocabulary knowledge and associated behavior, was used to assess the ICT security awareness level of participants. The development of the questionnaire is described in [5] and is only briefly repeated here.

The questionnaire consists of two sections; the first section is used to perform a vocabulary knowledge test, and the second to evaluate respondents' behavior. The questions in the first section consist of eleven general security concepts such as phishing, virus, spam etc. The selection of these concepts was based on information in the 2008 Information Security Breaches Survey conducted by PriceWaterhouseCoopers [8] and a SANS Institute report [9] on e-mail security threats. The

questions were constructed as multiple choice questions with five options to choose from. As an example, table 2 below shows the vocabulary test for the term *phishing* – it is expected that someone with a good understanding of phishing would select option (d) as the correct or most appropriate answer.

TABLE 2: EXAMPLE VOCABULARY TEST

Phishing is

(a) ☐ The use of an e-mail message, that appears to be legitimate, to solicit personal details
(b) ☐ Part of social engineering which means that someone is persuaded to give away confidential information
(c) ☐ Also referred to as identity theft
(d) ☐ All of the above
(e) ☐ I do not know what the term phishing mean

Section two of the questionnaire contained scenario type questions to evaluate respondents' behavior independently of their vocabulary knowledge. The majority of the questions were (with small adjustments) taken from a security awareness index report prepared during 2002 by Pentasafe Security Technologies [10]. The work of Furnell *et al* [11] was also used to construct some of the questions. A total of nine questions were asked to test the behavior linked to some of the concepts in section one of the questionnaire. For example, for the word *phishing* in section one of the questionnaire, the following scenario type question (see table 3) was used to test whether a respondent would withhold personal details irrespective of whether the respondent knew what the term *phishing* meant.

TABLE 3: EXAMPLE SCENARIO TYPE QUESTION

When receiving an e-mail that appears to be coming from your bank and asks you to go to a specific web link to confirm your personal details, what would you do? (select ALL that apply)

(a) ☐ If the bank's logo, address and all other information on the e-mail and webpage are correct, I will provide the required information
(b) ☐ I will simply ignore the request
(c) ☐ If my colleagues received the same request and if they had provided their details, I would do the same
(d) ☐ I would phone the bank to find out about the request
(e) ☐ I would report it to our company's IT department

Finally, to draw meaningful conclusions on the role of cultural factors in information security awareness, certain biographical questions were added to the questionnaire. Examples of some of the cultural questions include mother tongue, area where secondary schooling was completed (e.g. rural or urban area), type of secondary school attended (e.g. government or private school) etc.

The two universities where the experiment was conducted are both South African universities serving students from diverse backgrounds. They are both large and well established universities with more than one campus each. The one university has three different campuses with more than 50000 students while the other one has two campuses with more than 11000 students in total. The questionnaire was made available on the Internet to different selected class groups at the two universities and 180 useable responses were received. Figure 1 in Appendix A presents a demographic profile of the respondents.

The measuring instrument was validated by performing content validation and a reliability test.

Content validation is a process whereby items of a test are studied and weighted for their representativeness [12]. In this study content validity was established through relevant literature sources and the use of basic statistical tests such as correlations and contingency tables. The successful use of the instrument amongst students in a previous study [5] also supports the content validity.

Reliability refers to the accuracy or precision of a measuring instrument i.e. if the same set of objectives is measured again and again with the same instrument, will similar results be obtained? One way to assess this is to calculate a Cronbach alpha coefficient [12]. The Cronbach alpha coefficient for the eleven items in the questionnaire was 0.72 which was accepted as reasonable.

A complete validation of any measuring instrument normally includes a construct validation as well. Construct validity primarily answers questions such as what factors or constructs account for variance in test performance [12] and can be performed through a process called factor analysis. In this study construct validity was not performed as the questionnaire (vocabulary and behavior tests) has already been used successfully in a previous study amongst students [5].

IV. RESULTS AND DISCUSSION

Based on the results, it appears that certain of the cultural factors do have an effect on the security awareness of the students who participated in the survey. Before discussing these factors and their impact, a brief overview of the general findings pertaining to the vocabulary test will be given.

The majority of the respondents have a reasonable knowledge of threats linked to e-mail security such as *virus, spam, spyware* etc. They also appear to know what the concepts *strong password* and *hacker* mean. However, more than half of the students (54%) do not understand the term *security incident*. The most surprising result was the fact that social engineering and concepts linked to social engineering are not well known or understood by the respondents. Almost half of them (47%) answered that they do not know what the words *social engineering* mean while responses also indicate that they do not know what the associated concepts mean; almost 40% indicated that they do not know what *phishing* mean; 64% said that they do not know what *vishing* mean; and

60% do not know what *pharming* mean. What is encouraging in this case is that the scenario type questions (to test behaviour) related to social engineering show that most students will not easily reveal their personal information – even if they do not know what social engineering and the related concepts mean. Figure 2 below shows the responses to the scenario type question presented in table 2. The figures are presented as percentages and it should be noted that they do not add up to 100 as respondents may have selected more than one alternative.

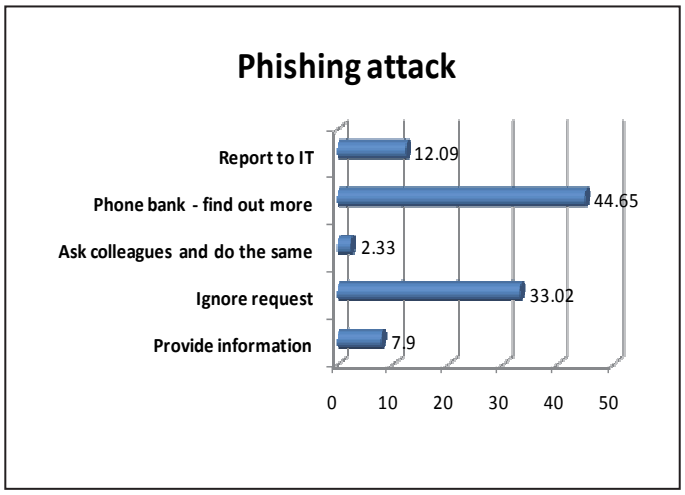


Figure 2: Reaction to possible phishing attacks

Not all results can be shown or discussed; therefore the two last graphs that show how respondents see ICT security and how they feel about information security are presented in figures 3 and 4 respectively.

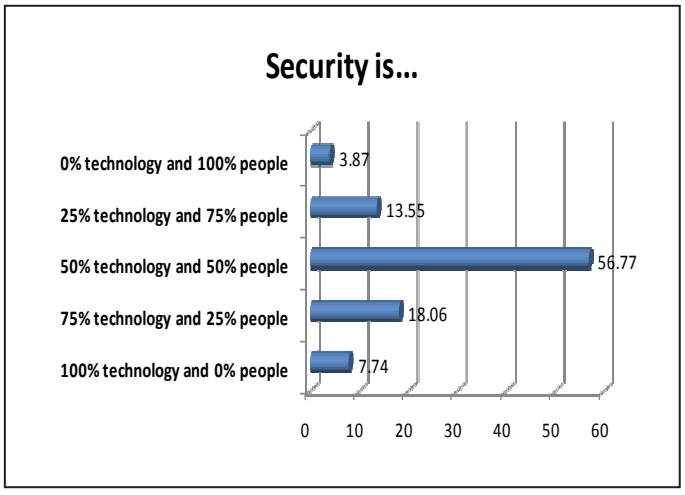
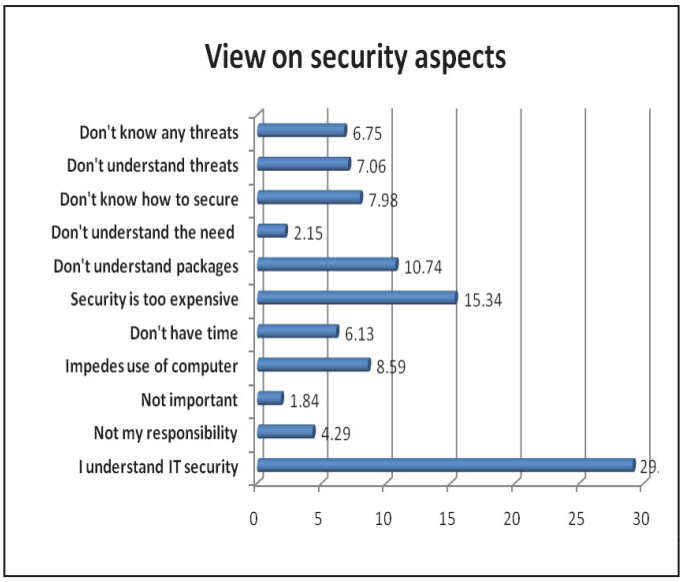


Figure 3: How respondents view security



To determine whether cultural differences among students have an effect on their ICT security awareness levels, certain basic statistical tests were performed. These tests included two-way analysis of variance (ANOVA) followed by Tukey post hoc tests. The ANOVA tests were used to determine if there was a statistical significance of the effects between each pair of factors and ICT security awareness level. It also indicates whether a significant interaction between them exists. The subsequent post hoc test was then used to determine the significance of differences in the mean scores between different levels of a factor.

The results of these statistical tests have shown that certain cultural factors do play an important role in security awareness levels of students. The main factors that may influence security awareness were found to be language (mother tongue) and the area where secondary schooling was completed (rural, peri-urban or urban). Other attributes that had, to a lesser extent, an impact include the number of years a respondent had access to a computer, the field of study and gender. The type of secondary school that was attended (government, former model C or private) did not play a significant role.

Due to paper length constraints a detailed discussion of all the cultural issues cannot be presented here. Figure 5 shows two tables that summarize some of the results categorized by the different language groups (language appeared to be the most significant cultural factor impacting the observed security awareness levels). The first table presents the results from the vocabulary test section while the second table gives information on some of the behavior tests found in section two of the questionnaire.

It can be seen from the first table in figure 5 (figure 5 follows at the end of the paper) that there are significant differences in the knowledge of security concepts amongst the various language groups. For example, 30% of language group 2, 25% of language group 1 and 27% of language group 4 (other) know what the term phishing mean while only 12% of language group 3 knows the meaning of phishing. Other significant differences, based on language groups, which can

be seen from the first table, include concepts such as spyware, worm, social engineering and so on.

The second table, which presents selected results from the behavior section, confirms the differences for the different language groups. There is, for example, quite a big difference between language group 1 and language group 2 in terms of password behavior. The same is true when one looks at the reported behavior when asked whether information will be provided in a social engineering scenario; only 6% of language group 1 is prepared to give away personal details while 24% and 29% of language groups 2 and 3 respectively will provide the information on request.

To summarize, the results obtained and described above show that firstly, the vocabulary test as part of the questionnaire used in this exercise was an acceptable way of evaluating ICT security awareness levels and that it could make a definite contribution to identifying specific areas for security education. Secondly, the results also indicated that cultural differences (especially mother tongue) amongst students may have an effect on their ICT security awareness levels.

For the specific case in this study, the results revealed the following.

- A security awareness program, for the students under discussion, should concentrate more on social engineering and the different terms and concepts related to it.
- Cultural differences, especially mother tongue, should be taken into account in any security awareness program. It may be necessary to concentrate on certain aspects for certain language groups while the same aspects may receive less attention for other language groups. Consideration should also be given to the use of more than one language in security awareness material. That does not mean that terms such as phishing should be translated, but rather that the concept and associated risks be presented and explained in the appropriate languages.

The results and the reported figures in this paper form part of an exploratory study and should not be regarded as a final comprehensive report or generalized results on cultural differences and ICT security awareness levels. Only a limited number of concepts were included in the vocabulary questionnaire; the sample size for the survey can also be expanded to include students from other universities and other language groups.

V. CONCLUSIONS

In this paper the traditional approach to an information security awareness program was extended to include possible cultural factors relating to people from diverse backgrounds.

A questionnaire consisting of a vocabulary test (to test knowledge) and a behavior test were used to assess security awareness levels of students at two different South African universities. As part of the biographical information, certain cultural questions (e.g. mother tongue, type of school attended etc.) were also included. The objective of these questions was to determine whether cultural differences among students have an effect on their security awareness levels. The results obtained suggested that certain cultural factors (especially mother tongue) do have an impact on security awareness levels and should be taken into consideration when planning and developing an information security awareness program.

REFERENCES

[1] J.F. Van Niekerk, Establishing an information security culture in organizations: An Outcomes Based Education Approach. MTech IT Dissertation. Nelson Mandela Metropolitan University, 2005.

[2] B. Schneier, Schneier on Security. New Jersey: John Wiley & Sons, 2008.

[3] K. Thomson and R. Von Solms, "Towards an Information Security Competence Maturity Model," Computer Fraud & Security, vol. 5, pp.11-15, 2006.

[4] G. Dhillon, Principles of Information Systems Security: text and cases. New Jersey: John Wiley & Sons, 2007.

[5] H.A. Kruger, L. Drevin, and T. Steyn, T. "A vocabulary test to assess information security awareness," Information Management & Computer Security, vol. 18(5), pp.316-327, 2010.

[6] I. V. S. Mullis, M. O. Martin, and P. Foy, "IEA's TIMMS 2003 International Report on Achievement in the Mathematics Cognitive Domains," International Association for the Evaluation of Educational Achievement (IEA), ISBN:1-889938-38-6, Boston College, 2005.

[7] M. S. Van der Walt, Aanpassing van die studie oriëntasievraelys in Wiskunde vir gebruik in die intermediêre fase. PhD dissertation. North-West University, 2008.

[8] PriceWaterhouseCoopers, Information Security Breaches Survey, Technical report. Available at www.security-survey.gov.uk. Accessed: 25 November 2009.

[9] SANS, E-mail Security Threats, SANS Institute InfoSec Reading Room, 2005.

[10] Pentasafe, Security Awareness Index Report: The state of security awareness among organizations worldwide, Pentasafe Security Technologies, 2002.

[11] S. M. Furnell, P. Bryant, and A. D. Phippen, "Assessing the security perceptions of personal Internet users," Computers & Security, vol. 26, pp.410-417, 2007.

[12] F. N. Kerlinger, Foundations of Behavioural Research. 3rd edition, CBS Publishing, Japan, 1986.

	Vocabulary concepts										
Language Group	**Phishing**	**Spyware**	**Virus**	**Worm**	**Spam**	**Password**	**Security incident**	**Hacker**	**Social engineering**	**Vishing**	**Pharming**
1	25	85	95	15	80	60	55	100	45	30	55
2	30	67	80	34	70	53	63	95	36	30	39
3	12	42	54	10	52	69	21	77	31	17	17
4	27	61	86	18	77	75	45	93	27	30	30

Note: Figures per language group are presented as percentages e.g. consider the Phishing column: 25% of language group 1 knows what phishing means

Table A

	Behavior		
	with respect to Passwords		with respect to Social Engineering
Language Group	**Memorize passwords**	**Will not give password away**	**Will provide info on request**
1	13	12	6
2	40	37	24
3	21	28	29
4	25	23	41

Note: Figures per language group are presented as percentages e.g. consider the Memorize Passwords column: 13% of those who indicated that they memorize their passwords belongs to language group 1

Table B

Figure 5: Selected results categorized by the different language groups

APPENDIX A

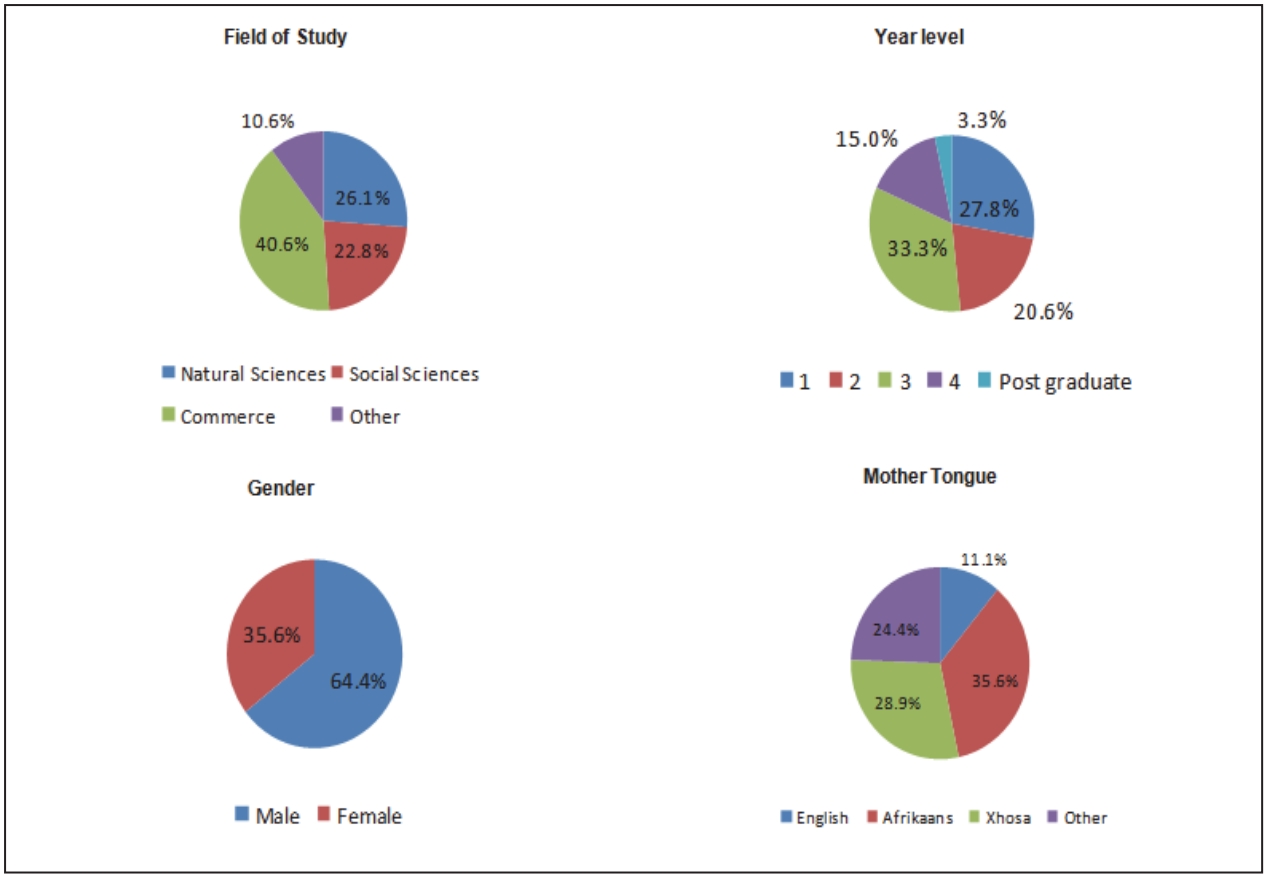


Figure 1: Demographic information of respondents