The Information Security Awareness of Bank Employees

M. Pattinson[1], M. Butavicius[2], K. Parsons[2], A. McCormac[2], D. Calic[2] and C. Jerram[1]

[1]Adelaide Business School, The University of Adelaide, Australia
[2]Defence Science and Technology Group, Edinburgh, Australia
e-mail: {malcolm.pattinson; cate.jerram}@adelaide.edu.au;
{marcus.butavicius; kathryn.parsons; agata.mccormac;
dragana.calic}@dsto.defence.gov.au

Abstract

This paper presents research that assessed the Information Security Awareness (ISA) of employees of an Australian bank and compared these results with an identical survey of the Australian general workforce. The objective of this study was to establish a form of construct validity, specifically known-groups validity, of the Human Aspects of Information Security Questionnaire (HAIS-Q). For the purposes of this study, ISA is a measure of an employee's knowledge of, and attitude towards, their organisation's Information Security (InfoSec) policies and procedures. This study used a web-based survey research method by utilising modules of the HAIS-Q. Individual knowledge and attitude were assessed for 198 bank employees and 500 general workforce participants. Seven InfoSec focus areas were evaluated: password management, email management, internet use, social media use, mobile computing, information handling and incident reporting. It was found that the levels of ISA for bank employees were approximately 20% better than those for the general workforce, in all InfoSec focus areas. Factors that may have contributed to this conclusive result are discussed and include social desirability bias; fear of reprisal; InfoSec education and in-house training.

Keywords

Information Security Awareness (ISA), Information Security (InfoSec), Social Desirability Bias, Fear of Reprisal.

1. Introduction

1.1. Background

This research focuses on assessing the Information Security Awareness (ISA) of employees, which is defined in this paper as being a combination of their knowledge of their organisation's Information Security (InfoSec) policies and procedures and their attitude towards having to comply with them. InfoSec policies and procedures typically contain statements or recommendations detailing how employees should behave in areas such as password management, internet use and incident reporting. More specifically, they will provide guidance on, for example, choosing a good password, accessing dubious websites and reporting bad behaviour of colleagues. Identifying the ISA of employees enables InfoSec management to develop effective methods to communicate and educate employees about organisational policies and procedures in those areas where ISA is assessed as being weak. This, in turn, has the potential to reduce the amount of risk-inclined computer-based behaviour and

therefore improve the security of the information assets of the organisation (Stanton, Mastrangelo, Stam & Jolton 2004; Trček, Trobec, Pavešsić & Tasič 2007).

This research used relevant modules of the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons, McCormac, Butavicius, Pattinson & Jerram 2014) to assess the knowledge and attitude of participants. This instrument was designed and developed as a modular tool to enable it to be tailored to specific research needs. For the research described in this paper, The Bank's Security Manager selected the knowledge and attitude modules and did not require self-reported behaviour information. This was a viable module choice as previous research has shown a strong relationship between knowledge, attitude and behaviour (Parsons et al. 2014), where knowledge and attitude have been shown to predict self-reported behaviour.

1.2. Research Aim

The aim of this research was to assess the Information Security Awareness (ISA) of employees of an Australian bank using the relevant modules of the HAIS-Q and to compare these results with the general workforce in Australia. The objective of this study was two-fold. Firstly, it would provide The Bank's InfoSec Management with information relating to the effectiveness of their current training and risk communication programs. Secondly, it would provide the researchers with evidence of a form of construct validity, specifically known-groups validity, of the HAIS-Q.

2. Justification for this Research

This research is predicated on the theory that employees with a higher level of ISA will be more risk-averse and therefore more compliant with organisational InfoSec policies and procedures. This will improve their computer-based behaviour and lead to a higher level of organisational InfoSec (Clarke, Symes, Saevanee & Furnell 2016). Hence, if employee ISA is known, intervention strategies such as training and education programs, can be implemented or modified to target the most vulnerable areas of awareness.

The results of this research project provided The Bank's InfoSec Managers with valuable information about the knowledge and attitude of employees, for the purposes of tailoring their InfoSec training programs. In addition, the InfoSec Managers were provided with a comparison of their employees' results with those of the general workforce. Their expectations prior to this research project were that the ISA of their employees should be higher than for the general workforce because bank employees are typically exposed to more sensitive and confidential information, and as a consequence, are usually better trained.

Another important reason for conducting this research was to further evaluate the construct validity of the HAIS-Q. Specifically, we evaluated 'known-groups validity' which is determined by the degree to which an instrument is sensitive to differences and similarities between groups (Hattie & Cooksey 1984). This was done by comparing the HAIS-Q scores of bank employees, who were expected to have higher scores, with the HAIS-Q scores of general workforce participants.

Known-groups validity testing is particularly useful when there is no gold standard psychometric measure to compare with.

3. Information Security Awareness (ISA)

Information Security Awareness (ISA) is a critical foundation for information security behaviour and compliance. Most definitions of ISA focus on two particular aspects of information security: understanding, and compliance. The first of these, understanding, refers to "the degree or extent to which every employee understands the importance of information security, the levels of information security appropriate to the organisation, [and] their individual security responsibilities" (Kruger & Kearney 2006 pp. 289). The second aspect, compliance, is concerned with the level of commitment to these InfoSec policies, rules and guidelines, exemplified by compliance (Kruger & Kearney 2006; Siponen 2001). Consequently, this paper interprets the above defintion of ISA as being a combination of an employee's knowledge of their organisation's Information Security (InfoSec) policies and procedures and their attitude towards having to comply with them.

4. Research Methods

4.1. Overview

The HAIS-Q (Parsons et al. 2014) was used to assess the ISA of employees at an Australian bank. The results were then compared to those of a previous research project that had assessed the Australian general workforce, also by using the HAIS-Q. For both studies, participants were asked to rate 21 statements relating to their knowledge of their organisation's InfoSec policies and procedures and 21 statements relating to their attitude towards these policies and procedures. These statements were presented on a 5-point rating scale ranging from 'Strongly disagree' to 'Strongly agree'. Three knowledge and three attitude statements were presented for each of the seven InfoSec focus areas, namely, password management, email use, internet use, social media use, mobile computing, information handling and incident reporting. Approximately half of the statements were negatively worded and statements across the seven InfoSec focus areas were randomly ordered. Negatively worded statements were taken into consideration prior to data analysis. Therefore, a participant's ISA score would be the sum of the number of occurrences of 'Strongly agree' and 'Agree' responses.

4.2. Surveys

For bank employees, 198 participants responded to a web-based questionnaire that was accessible via email from their respective work computers. This online version of the HAIS-Q was administered through the web-based survey software, Qualtrics. In addition to statements relating to participant knowledge of, and attitude towards InfoSec policies and procedures, participants were also asked to respond to demographic questions, questions about computer use and questions relating to personality and cognition.

For the general workforce participants, the same HAIS-Q was used to generate 500 valid responses from a wide range of participants in terms of their age, their job role and their employment industry. For more information about this survey, refer to Parsons et al. (2014).

5. Results

Table 1 below shows the percentage of favourable (that is, in line with policy) knowledge and attitude responses for both bank employees and general workforce participants. After reverse scoring, favourable responses were the sum of responses that were marked as either 'Strongly Agree' or 'Agree' and expressed as a percentage of the total number of responses for each InfoSec focus area.

Focus Area	Bank Employees			General Workforce		
	Knowledge	Attitude	ISA	Knowledge	Attitude	ISA
Password Management	77	89	83	55	67	61
Email Management	95	89	92	80	64.5	72
Internet Use	94	82	88	70	63	66.5
Social Media Use	92	89	90.5	71	80.5	76
Mobile Computing	92	94	93	63	67.5	65
Information Handling	96	97	96.5	75	75	75
Incident Reporting	88	89	88.5	70	67	68.5
Overall	90	90	90	69	69	69

Table 1: Percentage of Favourable Responses

The results show that the ISA percentage scores for bank employees are consistently 20% higher than those for the general workforce. This result holds true for all InfoSec focus areas as well as for the overall ISA percentage scores. This consistency is also reinforced by the fact that both groups recorded their lowest ISA scores for the Password Management focus area (83% and 61%) and high ISA scores for the Information Handling focus area (96.5% and 75%).

6. Discussion of Results

Although these results provide evidence for the construct validity of the HAIS-Q, further analyses of survey data have revealed a number of other factors that may have contributed to the results shown in Table 1 above. These are discussed below.

6.1. Social Desirability Bias

The HAIS-Q is administered with a short form of the Marlowe-Crowne Desirability Scale (Crowne & Marlowe 1960) to indicate the propensity of participants to respond

to questionnaire statements in a socially desirable manner. In other words, participants may be more inclined to respond in accordance with organisational policy and management expectations rather than tell the truth, and this scale is designed to capture this bias. The Marlowe-Crowne social desirability scale contains eight statements that each require a 'Yes', 'No' or 'Unsure' response. Respondents scored between zero and eight socially desirable answers (that is, 'Yes' selections). These scores were summed for both bank employees and general workforce participants and presented as a percentage of the total number of socially desirable statements for each population as shown in Figure 1 below.

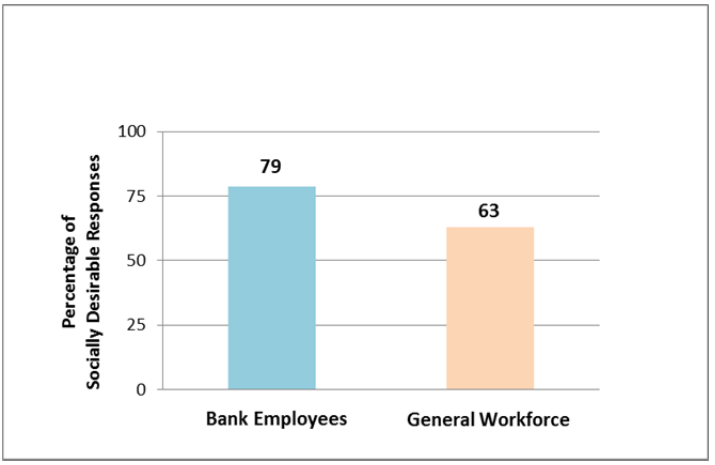

Figure 1: Social Desirability Bias

Based on these scores, bank employees responded in a more socially desirable manner compared to the general workforce participants. In other words, they may have been more likely to respond 'Yes' to the statement "*Are you always courteous even to people who are disagreeable?*" than general workforce participants. This could be assumed to indicate that their higher HAIS-Q scores are partly attributable to social desirability bias rather than higher ISA, but there are several mediating factors that must be considered before such conclusions can be drawn. As bank employees, their training and regular work environment practices would not only include a focus on client privacy and confidentiality, but would also include a heavy customer-service focus. Even more significantly, when responding to the HAIS-Q, the bank employees were actually at their work environment, as a workplace act, and would therefore be responding to the statements in a work context. In comparison, the general workforce participants principally answered the questions in their home or in a casual non-workplace environment. In summary, the real difference demonstrated in the social desirability scores between the two populations as shown in Figure 1 above, demonstrates consistency with the anticipated responses of well-trained bank employees. In other words social desirability bias is consistent with the higher levels of ISA of bank employees, and further strengthens the known-groups validity of the HAIS-Q.

6.2. Fear of Reprisal

In order to determine whether bank employees were more likely to respond in a socially desirable manner due to the work environment, their responses to two 'fear of reprisal' statements were also examined. Fear-of-reprisal statements are used in surveys, paper-based or online, to elicit a special type of a socially desirable response that provides an indication of whether participants are likely to be honest and, as a result, may jeopardise their employment or increase their risk of being penalised in some way. (Donaldson & Grant-Vallone 2002). For example, the statement "*Even though this questionnaire is confidential, I was still concerned that someone might identify my name with my responses?*" required a 'Yes', 'No' or 'Unsure' response. Participants' 'Yes' responses were totalled and presented as a percentage of the total number of fear-of-reprisal statements for each population.

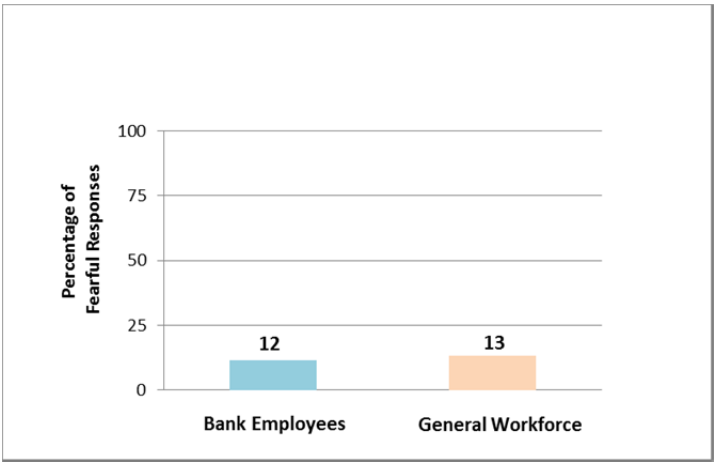

Figure 2: Fear of Reprisal

As shown in Figure 2 above, there was no substantial difference in the percentage of fearful answers for each group. Therefore, fear-of-reprisal responses do not appear to be a contributing factor to bank employees having a 20% higher level of ISA (when evaluated by using knowledge of, and attitude towards, policies and procedures) than general workforce participants. Hence, it is unlikely that bank employees responded in a more socially desirable manner due to fear of being penalised or disadvantaged. It is also unlikely that the customer-focussed environment of bank employees, compared to the general workforce, had much impact on their responses. For example, 91 (18%) of the 500 general workforce indicated that they worked in the area of "Customer Service". When these responses were extracted as a group, their knowledge, attitude and ISA results mirrored those of the rest of the general workforce.

6.3. Education and Training

In an attempt to explain the high levels of ISA of bank employees compared to general workforce participants, this research examined both the prior formal InfoSec education of all participants and the amount of workplace InfoSec training they had undertaken. Participants were asked "*Have you completed any university/TAFE subjects in the area of information security?*". A 'Yes' or 'No' response was required. The 'Yes' responses were totalled and presented as a percentage of the number of participants in each population.

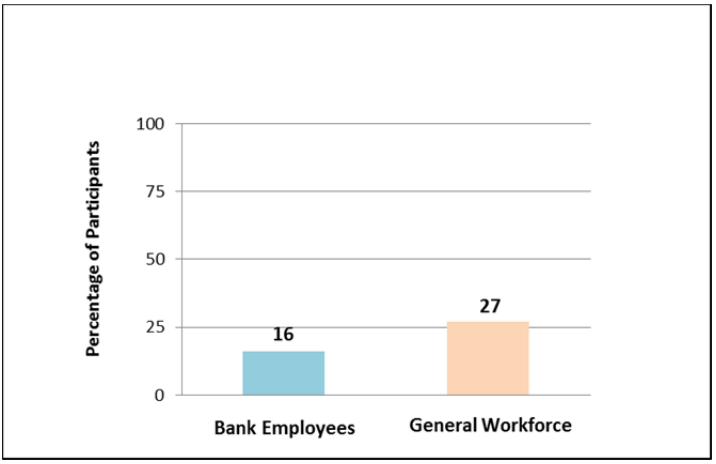

Figure 3: Formal InfoSec Courses Completed

As shown in Figure 3 above, 16% of the bank employees had completed a formal InfoSec course compared to 27% of the general workforce participants. This is a counter-intuitive result suggesting that more formal InfoSec education does not necessarily translate into a higher level of ISA. Previous research by Pattinson, Butavicius, Parsons, McCormac and Calic (2015) and Parsons, McCormac, Pattinson, Butavicius and Jerram (2013) is consistent with this result, reporting that people who have had more formal InfoSec education tend to be overconfident or complacent. This factor is likely to have contributed to the substantially higher ISA levels for the bank employees compared to the general workforce participants.

Participants were also asked "*How often have you undertaken information security training at work?*". A total of 14% (27) of the bank employees and 31% (155) of the general workforce participants had never completed any InfoSec training at work. This factor is likely to have had a major impact on the substantially higher ISA levels for the bank employees compared to the general workforce participants.

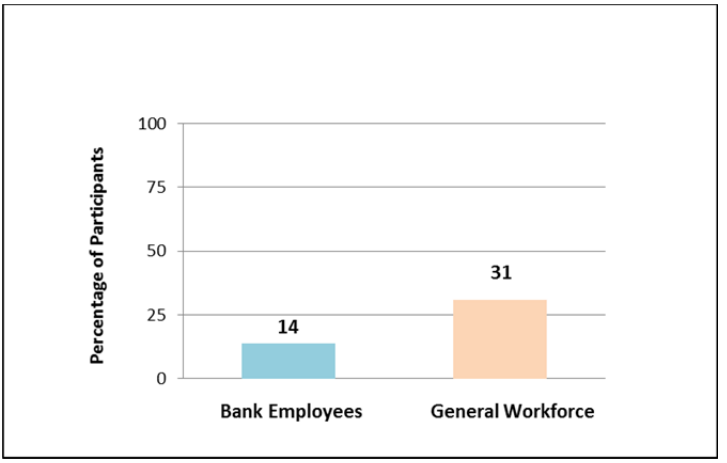

Figure 4: Never Completed any InfoSec Training at Work

To summarise, it appears that different types of education have different effects. On the one hand formal education can make people overconfident and complacent whilst focussed and specific training in a work environment can improve an employee's ISA.

7. Conclusions

The aim of the research project described in this paper was to compare the levels of ISA of bank employees with those of the general workforce, and in doing so, confirm a form of construct validity, called known-groups validity, of the HAIS-Q.

The levels of ISA of both bank employees and the general workforce participants were assessed by using only the knowledge and attitude modules of the HAIS-Q (and excluding the self-reported behaviour module). The results demonstrated that the average level of ISA for bank employees is approximately 20% higher than for the general workforce in all focus areas and overall.

Prior to this current research, it was anticipated that bank employees would have higher levels of ISA because of the sensitive nature of their organisation's information and therefore were more likely to have undertaken better InfoSec training. The results of this current research are consistent with these assumptions. This finding contributes to the construct validity of the HAIS-Q. Furthermore, bank employees were shown to have more propensity to give socially desirable responses (79%) compared to the general workforce participants (63%). However, this is likely to be a reflection of the work setting of bank employees compared to the non-work settings of the general workforce at the time of responding to the questionnaire.

In terms of fear-of-reprisal responses, there was very little difference between the bank employees and the general workforce participants. This result suggests that the

bank employees were not overly concerned about losing their job or being punished because they trusted the confidentiality and anonymity of their responses. However, the contextual issues with the use of the fear-of-reprisal statements has subsequently resulted in modifications to the HAIS-Q by introducing a few lie-scale statements (Donaldson & Grant-Vallone 2002) which will indicate whether a participant is responding truthfully or not.

To summarise, this study provided The Bank's InfoSec Management with evidence that their current InfoSec training programs and also the InfoSec culture within the organisation, was responsible for a substantially higher-than-average ISA for their employees. In addition, this study provided the researchers with evidence of a form of construct validity, specifically known-groups validity, of the HAIS-Q.

8. References

Clarke, N, Symes, J, Saevanee, H & Furnell, S 2016, 'Awareness of Mobile Device Security: A Survey of User's Attitudes', *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, vol. 7, no. 1, pp. 15-31.

Crowne, D & Marlowe, D 1960, 'A new scale of social desirability independent of psychopathology', *Journal of consulting psychology*, vol. 24, no. 4, p. 349.

Donaldson, S & Grant-Vallone, E 2002, 'Understanding self-report bias in organizational behavior research', *Journal of Business and Psychology*, vol. 17, no. 2, pp. 245-260.

Hattie, J & Cooksey, R 1984, 'Procedures for assessing the validities of tests using the" known-groups" method', *Applied Psychological Measurement*, vol. 8, no. 3, pp. 295-305.

Kruger, H & Kearney, W 2006, 'A prototype for assessing information security awareness', *Computers & Security*, vol. 25, no. 4, pp. 289-296.

Parsons, K, McCormac, A, Butavicius, M, Pattinson, M & Jerram, C 2014, 'Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security*, vol. 42, pp. 165-176.

Parsons, K, McCormac, A, Pattinson, M, Butavicius, M & Jerram, C 2013, 'Phishing for the truth: A scenario-based experiment of users' behavioural response to emails', in *Security and privacy protection in information processing systems*, Springer, pp. 366-378.

Pattinson, M, Butavicius, M, Parsons, K, McCormac, A & Calic, D 2015, 'Factors that Influence Information Security behaviour: An Australian Web-based Study', in T Tryfonas & I Askoxylakis (eds), *Human Aspects of Information Security, Privacy & Trust (HCI 2015),* Springer International, Los Angeles, vol. LNCS 9190, pp. 231-241.

Siponen, M 2001, 'Five Dimensions of Information Security Awareness', *Computers and society*, vol. 31, no. 2, pp. 24-29.

Stanton, J, Mastrangelo, P, Stam, K & Jolton, J 2004, 'Behavioral information security: two end user survey studies of motivation and security practices', in *Proceedings of the Tenth Americas Conference on Information Systems,* Citeseer, New York, USA, pp. 1388-1394.

Trček, D, Trobec, R, Pavešsić, N & Tasič, J 2007, 'Information systems security and human behaviour', *Behaviour & Information Technology*, vol. 26, no. 2, pp. 113-118.