An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations

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

[1]*Defence Science and Technology Organisation, Edinburgh, Australia*
[2]*Business School, University of Adelaide, Australia*

Abstract

This paper reports on a study conducted by The University of Adelaide with the support of the Defence Science and Technology Organisation, to examine information security (InfoSec) vulnerabilities caused by individuals, and expressed by their knowledge, attitude and behaviour. A total of 203 employees, from three large Australian government organisations, completed a web-based questionnaire designed to capture the knowledge, attitude and behaviour of individuals in regard to InfoSec. In conjunction with this employee questionnaire, qualitative interviews were conducted with a small number of senior management employees from each of the three organisations. Overall, the questionnaire results indicated that employees from all three organisations had reasonable levels of awareness of InfoSec vulnerabilities. Analysis of the qualitative interviews revealed that management not only had an accurate understanding of their employees' InfoSec awareness, but were able to recognise vulnerable areas that required further attention and improvement, such as the appropriate use of wireless technology, the reporting of security incidents and the use of social networking sites.

Keywords

Information security (InfoSec), InfoSec behaviour, Information Risk, InfoSec awareness, InfoSec vulnerabilities

1. Introduction

Management of InfoSec is a critical issue for both public and private sector organisations and there are growing expectations for organisations to ensure a high level of security of electronic data. Historically, problems with InfoSec have demanded a focus on technical solutions such as the development of hardware, software and network solutions. However, InfoSec is not only a technical problem, but is also a 'people' problem (Schultz, 2005). InfoSec-related issues can be better addressed by also considering the influence of the human factor to complement hardware and software solutions (Schneier, 2000).

The aim of this research project was twofold. The first aim was to gain a holistic understanding of the level of InfoSec awareness, defined by the dimensions knowledge, attitude and behaviour, of employees from Australian Government Organisations. The second aim was to develop and test an *Information Security Awareness Instrument* to assess the InfoSec awareness of employees. An inductive, qualitative approach was utilised in the development of the survey tool rather that the more commonly used theory verification approach (Karjalainen, 2011). This meant

that questions were developed before a model was applied, thus minimising the effect of bias (Karjalainen, 2011). This process formed the hypothesis that if computer users are in possession of adequate *knowledge* of InfoSec, this should result in a more positive *attitude* towards InfoSec, which should then result in more positive InfoSec *behaviour*. Hence, our three main dimensions of interest are knowledge, attitude and behaviour. This is sometimes referred to as the KAB model and has been studied in fields including InfoSec (Kruger & Kearney, 2006), climate change (van der Linden, 2012) and health promotion (Bettinghaus, 1986).

2. Method

2.1. Participants

Employees of three Australian Government organisations were invited via email to participate in a web-based questionnaire, and their participation was anonymous and voluntary. Response rates varied across the three organisations. In Organisation A, 123 of the 222 invited employees completed the questionnaire, resulting in a response rate of 55%. In Organisation B, 52 of the 200 invited employees completed the questionnaire, resulting in a response rate of approximately 26%. In Organisation C, 28 of the 746 invited employees completed the questionnaire, which equates to a response rate of approximately 4%. Hence, the overall response rate was approximately 17%.

It is important to highlight that the response rate of Organisation C is very low, which greatly affects the ability to generalise the findings. This means that the employees in Organisation C who chose to answer the questionnaire are likely to be systematically different from other employees of that organisation, and are essentially self-selected (Fowler, 2002). Fowler (2002) claims that self-selected participants in small sample sizes are more likely to have an interest in the topic in question. This means that the actual level of InfoSec awareness in Organisation C is likely to be lower than the level estimated by our study.

2.2. Web-based Questionnaire

The questionnaire was designed around eight aspects of InfoSec management:

- *Importance of InfoSec policies*,
- *Principles of InfoSec policies*,
- *Rules of InfoSec policies*,
- *Password management*,
- *Email and internet usage*,
- *Reporting security incidents*,
- *Consequences of behaviour* and *Training*.

These focus areas were chosen such that they allowed the researcher to identify any specific InfoSec weaknesses that could be subsequently addressed by management in the form of training, communication and policy development.

Participants were asked questions about their understanding of InfoSec threats and their experiences with InfoSec training within their organisation. More broadly, participants were asked to provide details about their general computer practices. Responses were used to produce measures of each of the eight focus areas along one or more of the dimensions: knowledge, attitude and behaviour.

Self-report questionnaires are often influenced by response bias and social desirability bias. Response pattern bias is observed when participants select the same response to every question. In order to eliminate and detect this behaviour, negatively worded questions were purposefully included in the questionnaire design. Social desirability bias is observed when individuals respond in a way that ensures they are seen to be behaving appropriately (Edwards, 1953). This bias, and the possible effects on results, is examined in more detail in the Discussion of this paper.

2.3. Management Interviews

To complement the questionnaire, qualitative interviews were conducted with members of senior management from each organisation. Three interviews were conducted with Organisation A, three interviews with Organisation B and two interviews with Organisation C. Each interview was conducted by two researchers with one member of senior management.

3. Results

3.1. Overview

Overall, the InfoSec awareness of employees who responded to the questionnaire was high. As mentioned previously, employee InfoSec awareness was assessed using three dimensions, namely, knowledge, attitude and behaviour. To provide more in-depth context specific information, the dimensions were divided into eight focus areas.

A number of questions were administered to provide a measure of each of these components, and Table 1 shows a summary of the results for each of the organisations. The mean score is shown with the standard deviation in brackets. Values range from ‘0’ to ‘1’ where ‘0’ represents the least appropriate response and ‘1’ the most desirable. Sample questions and results are also shown in Appendix A.

	Components	Organisation A	Organisation B	Organisation C	Total
Dimensions	Knowledge	0.92 (0.08)	0.86 (0.12)	0.91 (0.07)	0.90 (0.09)
	Attitude	0.86 (0.08)	0.76 (0.13)	0.86 (0.21)	0.83 (0.13)
	Behaviour	0.85 (0.08)	0.79 (0.09)	0.80 (0.09)	0.83 (0.09)
Focus Area	Importance of InfoSec policy	0.91 (0.09)	0.85 (0.16)	0.91 (0.22)	0.90 (0.13)
	Rules of InfoSec policy	0.87(0.08)	0.81 (0.10)	0.86 (0.13)	0.85 (0.10)
	Principles of InfoSec policy	0.92 (0.09)	0.85 (0.17)	0.90 (0.23)	0.90 (0.14)
	Password management	0.92 (0.10)	0.86 (0.12)	0.82 (0.11)	0.89 (0.11)
	Email and internet usage	0.88 (0.07)	0.83 (0.10)	0.90 (0.10)	0.87 (0.09)
	Report security incidents	0.71 (0.20)	0.65 (0.21)	0.70 (0.25)	0.69 (0.21)
	Consequences of behaviour	0.83 (0.12)	0.69 (0.16)	0.81 (0.21)	0.76 (0.16)
	Training	0.82 (0.14)	0.68 (0.16)	0.81 (0.26)	0.78 (0.17)

Table 1: Summary Results

It is important to highlight that this measure is still undergoing development, and has been completed by only 203 participants, who were not necessarily representative of the whole organisation. Hence, any comparisons between the organisations should be interpreted cautiously. For this reason, this report will only describe overall comparisons, based on the major dimensions of InfoSec awareness.

3.2. InfoSec Knowledge

In the section designed to capture knowledge about InfoSec, employees were provided with 15 statements. The purpose of these statements was to ascertain the employees' level of understanding of a number of important InfoSec rules. These statements addressed security considerations such as password selection, email and social networking site use, and using wireless technology to access information.

Participants could respond to each statement with either 'True', 'False' or 'Unsure', and the responses to each statement were assigned values from one to three. This assignment was such that, the more appropriate the response, the higher the value assigned to it, and a response of 'Unsure' was assigned a value of two (which is the middle value). Hence, for reverse questions, the scores were inverted, so that a higher score always corresponds with a better or more appropriate response.

The average scores were very high for the majority of the statements. All three organisations obtained average scores of 90% or higher for seven of the knowledge-based statements, and 80% or higher for a further six statements. This means that most employees had an appropriate knowledge of InfoSec. Results indicate that respondents had a good understanding of the importance of InfoSec rules, and had an

accurate knowledge of password security, and recognised that passwords should not consist solely of real words or significant dates or names.

Employees' knowledge of the security of wireless technologies was less convincing. As depicted in Appendix A, in response to the statement *"Wireless computing is considered to be less secure than wired computing"* the average score obtained by Organisation A was only 67%, and Organisations B and C had average scores of only 60% and 55%, respectively. Since wireless computing can pose a potential security risk, this is an area where education may be required.

In summary, the InfoSec knowledge demonstrated by respondents from Organisations A and C tended to be slightly higher than the knowledge demonstrated by Organisation B. However, this was usually only a difference of a few percentage points.

3.3. InfoSec Attitude

In the section assessing attitude towards InfoSec, employees were asked *"In terms of your work environment, how strongly do you agree with the following statements"*. Employees were asked to respond to 20 statements on a five-point scale from 'Strongly Disagree' to 'Strongly Agree'. The statements addressed areas such as the importance of InfoSec within their organisation, their exposure to training and their understanding of their responsibilities for maintaining InfoSec.

Employees' responses to each statement were assigned values from one to five. This assignment was such that, the more appropriate the response, the higher the value assigned to it. Hence, for reverse questions, the scores were inverted, so that a higher score always corresponds with a better or more appropriate response.

Employees of all organisations were judged to have a reasonable attitude towards InfoSec, with average scores for most variables at over 60%. The vast majority of employees from all three organisations recognised that their organisation has information that needs to be protected, believed that InfoSec is an important issue in their organisation, and recognised that it is important for them to act securely in all aspects of their work.

Generally speaking, employees from Organisations A and C were more likely to provide the most appropriate response than the employees from Organisation B. The largest difference between the organisations was obtained in response to the statement *"I believe that adequate security training is provided"*. Most participants from Organisation A and C agreed with this statement, with average scores of 75% and 78% respectively. In contrast, the average score obtained for Organisation B for this statement was only 49%.

There was also a large variation in response to the statement *"What I do on social networking sites is none of my employer's business"*. The vast majority of employees from Organisation C recognised that their behaviour on these sites is of some interest to their employer, with an average score of 79%, whereas the average scores

provided by Organisations A and B were only 58% and 59%, respectively. Since social networking sites can have numerous negative consequences, such as jeopardising the security, confidentiality and reputation of an organisation (Parsons, McCormac & Butavicius, 2011), this is therefore an area where education may be required for employees from Organisations A and B.

3.4. InfoSec Behaviour

In the section assessing InfoSec behaviour, participants were provided with 16 statements and were asked to indicate how frequently they engaged in certain behaviours, both conducive and detrimental to InfoSec. Examples include, *"I delete suspicious emails"*, *"I share my password with others"*, and *"I open attachments from unknown sources"*. Participants were asked to respond on a five-point scale, from 'Never' to 'Always', and the responses to each statement were assigned values from one to five. This assignment was such that, the more appropriate the response, the higher the value assigned to it.

In summary, self-reported behaviour of employees from all organisations was considered reasonable, with an average score for most questions of 70% or higher. Although there was some variation across the questions, generally speaking, the respondents from Organisation A were most likely to respond appropriately, and the employees from Organisation B were less likely to do so.

The vast majority of employees from all organisations reported that they never share their passwords with others, and would never download non-corporate software or music or video content from the Internet onto their work computers. Although most employees from Organisation A would not use a USB stick to transfer files between work and home, a number of employees from Organisations B and C admitted that they sometimes do so.

Results also indicated that many people do not keep a clear and tidy desk at work, and there were also areas associated with reporting of security incidents where people did not respond appropriately. For example, in response to the statement *"If I see unfamiliar people in my office area I will approach them and ask to see their identification,"* employees from Organisation A scored an average of 56%, Organisation B scored an average of 49% and Organisation C scored an average of 69%. The response to this statement must be examined in light of the organisation in question. Some organisations have a policy where visitors must be escorted, and therefore, it is not appropriate for someone to approach an escorted visitor, but it would be necessary to approach an unfamiliar person if the individual in question is not being escorted.

3.5. Management Interviews

To determine whether management within the three organisations had a good understanding of the InfoSec awareness of their employees, members of senior management from each organisation were interviewed. A total of eight interviews were carried out. Although the interviewees all held senior management positions

within their organisations, some were responsible for day-to-day operations and people management, whereas others were specifically responsible for InfoSec management.

A semi-structured interview technique was utilised, and the interviews included questions regarding InfoSec policy, procedures, culture and management attitude towards InfoSec.

Generally, the information provided by the senior managers of all three organisations was consistent with the responses from the employees of their organisations, indicating that management have a good understanding of the InfoSec awareness of their employees. Essentially, management believed that most employees have an appropriate level of InfoSec awareness, but recognised that there were areas of improvement required.

The managers had a very good knowledge not only of the InfoSec policies of their organisation, but also understood what constituted good InfoSec management in general. The managers recognised that there can be tensions between the necessity to abide by any security regulations and the need to get the job done. They also explained that there can be challenges associated with keeping any InfoSec policy current with so many fast changing technological advances.

However, the managers believed that most employees have a sense of responsibility and professionalism for the information held by their organisation. Therefore, managers believed that security breaches would be more likely to be caused by unintentional lapses rather than maliciousness. Managers believe that this was particularly true of employees who had been with the organisation for some time, as this sense of responsibility and professionalism is stronger once employees have been enculturated within the organisation. With new employees, the managers of all organisations explained that a greater emphasis is placed on punitive measures.

All managers also acknowledged that their organisation has potential vulnerabilities associated with the use of social networking sites, and although the potential risks associated with these sites should be covered by current policies associated with Internet usage and general privacy or confidentiality rules, the managers still acknowledged that this is an area where further education is required to emphasise the possible risks, and reinforce the restrictions on use.

In summary, the results of the management interviews support the findings from the employee questionnaires. Essentially, managers recognised that there were some weaknesses with regards to InfoSec awareness, training and compliance, but generally believed that most employees at their organisation have a reasonable level of InfoSec awareness.

4. Discussion

Interviews were conducted with members of senior management from three organisations, and employees of these organisations were asked to complete a web-based questionnaire, which contained questions relating to demographic details, perceived information risks, knowledge of information security policies, information security attitudes, and behaviour whilst using a computer.

The results of this survey indicate that the level of awareness of employees within all three organisations was generally satisfactory. Overall, answers to questions relating to knowledge received higher scores than those for attitude and behaviour. A summary of the most important findings is provided below:

- The InfoSec knowledge of employees was very good. Employees from all organisations scored 90% or higher in response to seven knowledge-based statements, and 80% or higher in response to a further six statements. Respondents had a good understanding of the importance of InfoSec rules, and had an accurate knowledge of password security, and recognised that passwords should not contain only real words or significant dates or names. There were, however, some aspects of wireless technology where many employees lacked knowledge.

- Most respondents also had a good attitude towards InfoSec. However, in general, the scores for their attitude-based questions were slightly lower than those based on their knowledge. Employees generally recognised that their organisation has information that needs to be protected, believed that InfoSec is an important issue in their organisation, and recognised that it is important for them to act securely in all aspects of their work. However, responses indicated that Organisation B may need to improve their InfoSec training, and all organisations may need to educate employees about the use of social networking sites.

- Reported employee behaviour was also good. Overall, scores for the behaviour-based questions were similar to those testing their attitude. Most employees stated that they would never share their passwords with others, and would never download non-corporate software or music or video content from the Internet onto their work computers. However, people were far less likely to keep a clear and tidy desk, and there were areas associated with the reporting of security incidents where people did not respond appropriately. In addition, while most employees from Organisation A knew not to use a USB stick (thumb drive) to transfer files between work and home, a number of employees from Organisations B and C admitted that they sometimes do so.

- Interviews with senior management revealed that the managers had a good understanding of the InfoSec awareness of their employees, and understood what constituted good InfoSec management in general. However, they also acknowledged some areas of concern such as the need for more education in the appropriate use of social networking sites whilst at work.

It is important to highlight that the data from Organisation C is based on only 28 employees due to a very poor response rate. It is likely that those who chose to respond are systematically different from the employees who did not participate in the questionnaire which greatly affects the generalisability of the findings from this organisation.

There are a number of possible limitations associated with this research. For example, the results of this report are based on self-report which does not always reflect true attitudes and behaviour, as some respondents may be influenced by biases. For example, according to the social desirability bias, respondents may consciously or unconsciously answer in a way that ensures that they are presented in a positive light (Edwards, 1953). However, previous research has shown that an individual's perceptions, attitudes and knowledge can be appropriately measured via self-report (Schmitt, 1994; Spector, 1994). Additionally, to further decrease the influence of this bias, and increase the chance that employees responded openly about InfoSec awareness, employees were informed that the survey was being conducted anonymously.

5. Conclusions and Future Research

In general, participants scored slightly higher on questions testing their knowledge than for those regarding behaviour and attitude. While it is difficult to compare scores directly across these three areas, this finding is nonetheless consistent with the sentiment echoed by the managers in their interviews; namely, that employees generally possessed good knowledge of InfoSec even if their actions were not always consistent with good policy. This suggests that any remedial action might be best directed towards training programs to improve policy compliance that focus on changing the behaviour of participants. This training should be contextualised (i.e., tailored to the specific needs of the audience) and use case studies (Brooke, 2006) rather than generic courses that resemble lectures in order to improve compliance with, rather than simply knowledge of, policy (Parsons, McCormac, Butavicius, & Ferguson, 2010). In particular, as evidenced with both questionnaire participants and management interviewees, the use of social networking sites is still a potential issue and specialised training programs may be beneficial (Parsons et al., 2011).

The next stage of research will examine the effectiveness of various training and risk communication options by using the questionnaire developed in this current research in a pre-test/post-test methodology. For example, the authors are interested in developing e-simulation scenarios and comparing the effectiveness of this form of training with more traditional methods such as lectures. Furthermore, the authors intend to refine the questionnaire presented in this report so that it can be used as the basis of benchmarking the state of information security within various industries. The questionnaire could also be used to track the long-term InfoSec health of an organisation over a significant period of time (Wilson & Hash, 2003).

6. References

Bettinghaus, E. P. (1986), “Health promotion and the knowledge-attitude-behavior continuum”, *Preventive Medicine*, Vol. 15, No. 5, pp475-491.

Brooke, S. L. (2006), "Using the case method to teach online classes: Promoting Socratic dialogue and critical thinking skills", *International Journal of Teaching and Learning in Higher Education*, Vol. 18, No. 2, pp142-149.

Edwards, A. L. (1953), "The relationship between the judged desirability of a trait and the probability that the trait will be endorsed", *Journal of Applied Psychology*, Vol. 37, No. 2, pp90-93.

Fowler, F. J. (2002), *Survey Research Methods (3rd ed.)*, Sage, Thousand Oaks, CA, ISBN: 1412958415

Karjalainen, M. (2011), *Improving Employees' Information Systems (IS) Security Behaviour: Toward a Meta-Theory of IS Security Training and a New Framework for Understanding Employees' IS Security Behaviour*, PhD, University of Oulu, Oulu. (A 579)

Kruger, H., & Kearney, W. (2006), "A prototype for assessing information security awareness", *Computers & Security*, Vol. 25, No. 4, pp289-296.

Parsons, K., McCormac, A., & Butavicius, M. (2011), *Don't Judge a (Face) Book by its Cover: A critical review of the implications of social networking sites*, Defence Science & Technology Organisation, DSTO-TR-2549.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010), *Human Factors and Information Security: Individual, Culture and Security Environment*, Defence Science and Technology Organisation, DSTO-TR-2484.

Schneier, B. (2000), *Secrets and lies: digital security in a networked world*: Wiley, ISBN: 0-471-25311-1.

Schmitt, N. (1994), ‘Method bias: The importance of theory and measurement’, *Journal of Organizational Behavior*, Vol. 15, pp393-398

Schultz, E. (2005), ‘The human factor in security’, *Computers & Security*, Vol. 24, No. 6, pp425-426.

Spector, P.E. (1994), ‘Using self-report questionnaires in OB research: A comment on the use of a controversial method’, *Journal of Organizational Behavior*, Vol. 15, p385-392.

van der Linden, S. (2012, July), Understanding and achieving behavioural change: Towards a new model for communicating information about climate change. Paper presented at the *International Workshop on Psychological and Behavioural Approaches to Understanding and Governing Sustainable Tourism Mobility*, Freiburg, Germany.

Wilson, M. & Hash, J. (2003), *Computer Security: Building an Information Technology Awareness and Training Program*, NIST SP: 800-50.

Appendix A

Please indicate whether these statements are true or false.

	True	False	Unsure
Wireless computing is considered to be less secure than wired computing	○	○	○

In terms of your work environment, how strongly do you agree with the following statements?

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I believe that adequate security training is provided	○	○	○	○	○
What I do on social networking sites is none of my employer's business	○	○	○	○	○

Please indicate how frequently the following statements apply to you when you are at work.

	Never 1	2	3	4	Always 5
I share my password with others	○	○	○	○	○
If I see unfamiliar people in my office area I will approach them and ask to see their identification	○	○	○	○	○
I open attachments from unknown sources	○	○	○	○	○

Figure A: Screenshot of sample questions as shown to participants

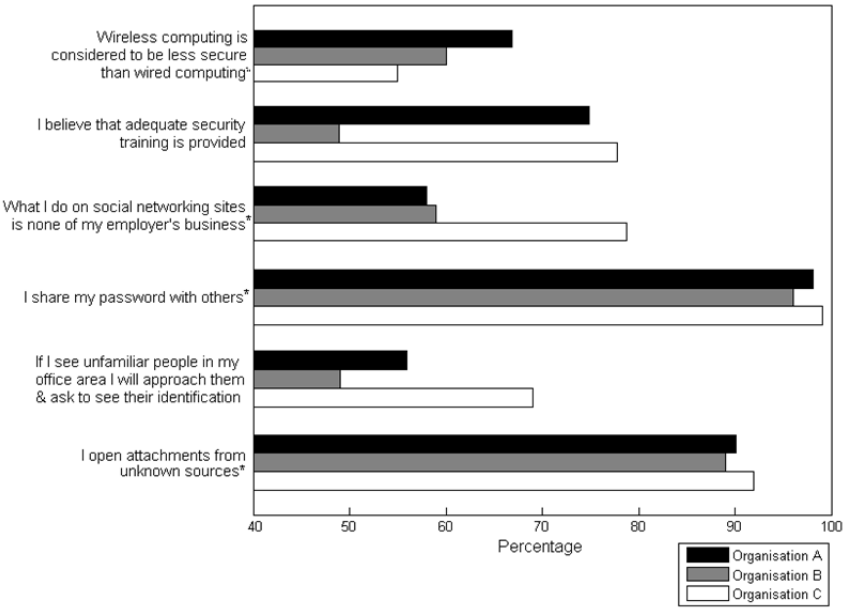

Figure B: Results of sample questions for each organisation