Received 29 January 2016
Revised 29 January 2016
Accepted 9 March 2016

Assessing information security attitudes: a comparison of two studies

Malcolm Pattinson
Business School, The University of Adelaide, Adelaide, Australia, and
Kathryn Parsons, Marcus Butavicius, Agata McCormac and Dragana Calic
Defence Science and Technology Organisation, Edinburgh, Australia

Abstract

Purpose – The purpose of this paper is to report on the use of two studies that assessed the attitudes of typical computer users. The aim of the research was to compare a self-reporting online survey with a set of one-on-one repertory grid technique interviews. More specifically, this research focussed on participant attitudes toward naive and accidental information security behaviours.

Design/methodology/approach – In the first study, 23 university students responded to an online survey within a university laboratory setting that captured their attitudes toward behaviours in each of seven focus areas. In the second study, the same students participated in a one-on-one repertory grid technique interview that elicited their attitudes toward the same seven behaviours. Results were analysed using Spearman correlations.

Findings – There were significant correlations for three of the seven behaviours, although attitudes relating to password management, use of social networking sites, information handling and reporting of security incidents were not significantly correlated.

Research limitations/implications – The small sample size ($n = 23$) and the fact that participants were not necessarily representative of typical employees, may have impacted on the results.

Practical implications – This study contributes to the challenge of developing a reliable instrument that will assess individual InfoSec awareness. Senior management will be better placed to design intervention strategies, such as training and education of employees, if individual attitudes are known. This, in turn, will reduce risk-inclined behaviour and a more secure organisation.

Originality/value – The literature review indicates that this study addresses a genuine gap in the research.

Keywords Theory of planned behaviour, Information security (InfoSec), InfoSec behaviour, Repertory grid technique (RGT)

Paper type Research paper

1. Introduction

1.1 Background

There is a growing body of literature (Parsons *et al.*, 2014; Pattinson and Anderson, 2007; Schneier, 2004; Stanton *et al.*, 2005; Trček *et al.*, 2007; Vroom and von Solms, 2004) that asserts that a more effective means of reducing information risk within an organisation is to address the behaviour of computer users in parallel with, and not

Information & Computer Security
Vol. 24 No. 2, 2016
pp. 228-240
Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-01-2016-0009

instead of, addressing hardware and software vulnerabilities. This behavioural approach to managing information security (InfoSec) supports Schneier's (2004) claim that "[…] the biggest security vulnerability is still that link between keyboard and chair" (p. 1).

As a result, management are starting to focus on behavioural solutions to achieve the purported benefits that a positive change in computer user behaviour can have on the security of their computer systems. In an extensive literature review, Abraham (2011) cites a paper by Thomson and von Solms (1998) as one of a small number of studies that acknowledge the importance of computer users' attitudes in refining InfoSec behaviour.

The research described in this current paper focuses on behavioural InfoSec. More specifically, it examines the attitudes that computer users have towards naïve and accidental behaviour. Examples of naïve and accidental behaviour include: leaving a computer unattended; opening unsolicited email attachments; using guessable passwords; not reporting security incidents; and accessing dubious web sites.

1.2 Aims

The aim of this research was to compare two studies that assessed the attitudes of typical computer users toward naïve and accidental InfoSec behaviour. The first study used a quantitative self-reporting online survey instrument and the second study used a set of Repertory Grid Technique (RGT) interviews.

The structure of this paper is as follows. The next section provides the justification for this research and is followed by a summary of the most relevant literature and the theories that underpin the research. The two studies are then described and the results are presented and summarised. Finally, the limitations of this research, the conclusions and future directions are discussed.

2. Justification for this research

This current research is motivated by the need to understand the attitudes of employees toward InfoSec behaviours (Ajzen, 1991; McGuire, 1969). This will enable the implementation of appropriate intervention strategies to improve knowledge and attitudes to minimise risk-inclined behaviour. Figure 1 below shows the logic hierarchy of how this will lead to a higher level of security of the information system assets within an organisation.

Furthermore, Crossler *et al.* (2013) highlight the need for future behavioural InfoSec research that addresses better methods of collecting, eliciting and measuring security-related data, particularly attitude data. These authors also call for research that differentiates between insider deviant behaviour and insider misbehaviour. The research described in this paper addresses both of these requests by comparing two methods of capturing attitude data, namely, a quantitative self-reporting online survey and a set of qualitative interviews. In addition, this paper focuses on insider misbehaviour and refers to it as naïve and accidental behaviour.

Figure 1.
Logic hierarchy of this current research

3. Theoretical issues and literature

3.1 Overview

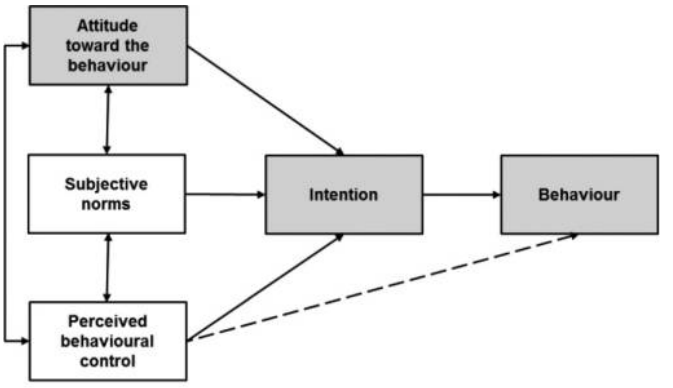
Although there are many publications relating to the interaction between humans and computer systems [commonly known as human-computer interaction (HCI)] (Myers *et al.*, 1996; Olson and Olson, 2003; Parsons *et al.*, 2014; Zhang *et al.*, 2002), there is very little rigorous research devoted to factors that may influence safe/unsafe user behaviour relating to computer use. Only recently has literature emerged out of the InfoSec discipline that considers the impact of individual behaviour whilst using a computer (Leach, 2003; Parsons *et al.*, 2014; Stanton *et al.*, 2005; Trček *et al.*, 2007).

The theoretical framework that underpins this current research is a component of Ajzen's (1991) theory of planned behaviour (TPB) that claims that attitude towards behaviour is positively associated with intended behaviour. (Refer the shaded areas in Figure 2 below.) The other antecedents of the TPB that are claimed to influence intended behaviour include subjective norms and perceived behavioural control (non-shaded areas); however, these are not within the scope of this study.

Many studies (Furnell *et al.*, 2006; Kruger and Kearney, 2006; Stanton *et al.*, 2005) have been conducted since Fishbein and Ajzen (1975) and Ajzen (1991) developed the theories of reasoned action (TRA) and TPB in an attempt to understand peoples' intentions to engage in a variety of InfoSec activities. These theories are based on the assumption that intentional behaviour is directly related to actual behaviour (Fishbein and Ajzen, 1975).

3.2 Human behaviour

The disciplines of social psychology and economics have generated a large amount of literature, research and knowledge relating to behaviour within organisations. In these studies, numerous theories have been put forward, many statistics have been analysed and reported on and many concepts and principles have been developed. Examples are the risk homeostasis theory (Wilde, 1994, 1998), the bystander effect theory (Darley and Latane, 1968), the theory of reasoned action (Ajzen and Fishbein, 1973) and the theory of planned behaviour (Ajzen, 1991), to name a few. However, these studies have largely ignored the behaviour of people when they are working at a computer, particularly naïve



Note: Shaded areas indicate the scope of this research

Figure 2.
Theory of planned behaviour

and accidental behaviour that relates to the security of an organisation's information systems.

3.2.1 Information security (InfoSec) behaviour. InfoSec behaviours have been categorised in different ways by numerous studies (Parsons *et al.*, 2014; Pattinson and Anderson, 2007; Stanton *et al.*, 2005). For example, Stanton *et al.* (2005) refer to risk-averse behaviours as "Aware Assurance" or "Basic Hygiene"; naïve behaviours as "Dangerous Tinkering" or "Naïve Mistakes"; and risk-inclined behaviours as "Intentional Destruction" or "Detrimental Misuse". The term "InfoSec behaviour" usually refers to the full spectrum of behaviours by people who make significant use of computers as part of their job. As shown in Table I below, these behaviours range from deliberate risk-averse behaviours to deliberate risk-inclined behaviours. However, the research described in this paper is focussed only on naïve and accidental behaviours, as shown below.

3.3 Attitude towards behaviour

Although the concept of "attitude" is both complex and has been defined in many different ways (Schrader and Lawless, 2004), the psychology literature has essentially reached agreement on the concept of "attitude toward behaviour" or at least toward intended behaviour generally. Attitude is universally understood as an overall feeling of a behaviour being favourable or unfavourable (Ajzen and Fishbein, 2000). Other commonly used descriptions include: behaviour that is liked or disliked; desirable or undesirable; good or bad; or behaviour that is viewed positively or negatively. For the purposes of this paper, attitudes toward InfoSec behaviour are conceptualised in terms of the extent to which a behaviour has the potential to put an organisation's information assets at risk. In other words, is the behaviour considered to be safe or unsafe, less risky or more risky or likely to cause a low impact or a high impact?

Deliberate risk-averse behaviours	Naive and accidental behaviours	Deliberate risk-inclined behaviours
Always log-off when computer unattended	Leaving a computer unattended	Installing/using unauthorised software
Disallow email attachments from unknown sources	Opening unsolicited email attachments	Create and send spam email
Install more than one anti-virus software package and update regularly	Not installing anti-virus software	Writing and disseminating malicious code
Change password regularly	Sharing ID's and passwords	Hacking into other people's accounts
Vigilant in recognising and approaching unauthorised personnel	Not being vigilant of unauthorised personnel	Giving unauthorised personnel access to authorised precincts
Back up work regularly	Not backing up work often enough	Theft or destruction of hardware or software
Always report security incidents	Not reporting security incidents	Conducting fraudulent activities
Install firewall	Accessing dubious web sites	Executing games on company equipment

Table I. Examples of InfoSec behaviours (Pattinson and Anderson, 2007)

3.4 Repertory grid technique (RGT)

The RGT is a cognitive technique developed by, and grounded in, Kelly's (1955) personal construct theory. It is a method of interviewing in which interview participants divulge their perceptions, thoughts and views about a particular situation, object or event. The RGT has been used for a variety of applications within different domains such as psychology research (Armsby *et al.*, 1989; Bannister, 1981) and in management research (Tan, 1999). The RGT has also been applied in the information technology domain by Tan and Hunter (2002) who used it to investigate "the personal constructs that users and IS [information systems] professionals use to interpret IT [information technology] and its role in organizations" (p. 53). Similarly, Whyte *et al.* (1996) used the RGT to analyse factors that affect information systems "success". They interviewed business people and elicited their thoughts and opinions regarding factors that contribute to the "success" of the information systems they use.

Kelly's (1955) personal construct theory and the RGT are ideally suited to the qualitative nature of the information being sought, namely, attitudes. This argument is supported by Hair *et al.* (2009) who conclude that the RGT was an excellent tool to use within qualitative interviews because it enabled the elicitation of both hidden as well as tacit knowledge from interviewees. Other reported advantages of the RGT are that it can keep socially desirable responses to a minimum (Fransella *et al.*, 2004) and minimise researcher bias (Jankowicz, 2004). The RGT is also advantageous compared to other elicitation techniques because it facilitates both qualitative and quantitative data analysis (Curtis *et al.*, 2008).

4. Research

4.1 Overview

This research project consisted of two studies that assessed the attitude of computer users toward a selection of naïve and accidental, InfoSec behaviours. Participants were university students who were recruited via email. The demographics of the sample of 23 participants are shown in Table II below.

4.2 Study 1: online survey questionnaire

In this study, 23 students completed a web-based survey within a university laboratory setting. This online Qualtrics questionnaire consisted of demographic questions; computer usage questions; personality and cognitive questions; and knowledge, attitude and behaviour questions. Refer Parsons *et al.* (2014) for a more detailed explanation of this survey. The survey took approximately 40 min to complete for which participants were paid US$30.

Participants were asked to rate their attitude towards the seven computer-based behaviours shown in Table III below. A five-point rating scale ranging from "Strongly disagree" to "Strongly agree" was used. Negative statements were reversed prior to analysis.

4.3 Study 2: repertory grid technique (RGT) interviews

For this study, the same 23 participants were interviewed by the researcher using the RGT. The objective of these semi-structured interviews was to elicit the thoughts and views pertaining to their attitude toward the same seven InfoSec behaviours that were used in the online questionnaire. Each interview took approximately 45 min, and each participant was paid a further US$30 for their participation.

Gender	
Male	11
Female	12
Age	
19 or under	7
20-29	12
30-39	3
40-49	1
50-59	0
60 or over	0
Employment status	
Currently employed	11
Currently unemployed but with previous experience	8
Currently unemployed with no previous experience	4
Current level of university	
First year	7
Second year	3
Third year	4
Fourth year	3
Post-graduate	6
Highest level of education completed	
Did not graduate from high school	0
Year 12 or equivalent	13
Some post-secondary	1
Bachelor degree	8
Post-graduate degree	1

Table II. Participant demographics

Focus area	Statement
Password management	It is a good idea to use a strong password
Email use	I take a big risk if I open an email attachment from a completely unknown sender
Internet use	My university should not check what internet content I access when I am using their network in my own time
Social networking	It is a bad idea to post sensitive university information on Facebook
Mobile computing	If I access sensitive university research data on a laptop in a public place, it does not matter if people can see my screen
Information handling	Nothing bad will happen if I insert an unknown USB flash drive into a university computer
Incident reporting	It is important for me to report security incidents because, even if I think it is not significant, it could have security implications

Table III. Statements of attitude towards InfoSec behaviour

For these RGT interviews, a set of elements was required that represented the research topic of interest, which was "Attitudes toward information security behaviours". These elements were all risk-inclined, naïve and accidental behaviours. The RGT interviews were then conducted with the supplied elements for the sole purpose of eliciting bi-polar

constructs from interviewees that represented their thoughts, views and attitude towards each of the InfoSec naïve and accidental behaviours. This method uses the techniques of triading, laddering and pyramiding to extract appropriate and useful information from interviewees whilst ensuring researcher bias is eliminated and socially desirable responses are minimised (Stewart *et al.*, 1981). Interviewees were specifically asked "What word or phrase would you use to describe the behaviour". On average, eight bi-polar constructs were rated by each participant before saturation was reached.

Figure 3 below shows a typical filled-in RGT individual interview sheet with the seven elements as columns and (in this case) eight elicited bi-polar constructs as rows (construct number 10 was supplied by the researcher). The 7 × 9 matrix of numbers are the element-construct scores out of 5 whereby "1" represents the left-hand side construct and "5" represents the right-hand side construct. For example, in Figure 3 below, the interviewee thought that behaviour number 6, "Inserting an unfamiliar DVD or USB into a Uni computer" was relatively "Less harmful to information" compared to the other six behaviours and therefore scored it a "4", as shown circled in red.

The set of 23 repertory grids consisting of 188 constructs needed to be reduced into a more manageable set of attitudes, and this was done via a formal categorisation process in accordance with Jankowicz's (2004) core categorisation method. To analyse the raw grid data in a grounded theory manner, a set of themes (i.e. categories) were developed (Cassell and Walsh, 2004). This research adopted the Osgood *et al.* (1957) three basic dimensions of responses to semantic differential constructs to assess attitude. The three dimensions, namely, evaluation, potency and activity (EPA) have been used extensively, in particular, in studies about attitudes (Heise, 1970; Kervyn *et al.*, 2013). For this current study, the constructs were categorised as:

- *Evaluation (E)*: If the construct refers to behaviours as being good-bad, accidental-deliberate, sensible-foolish, responsible-careless, etc.

REPERTORY GRID INTERVIEW 1	1. Using weak, guessable passwords	2. Opening email attachments from unknown senders	3. Viewing inappropriate web sites on a Uni computer	4. Posting sensitive Uni Information on FaceBook using a Uni computer	5. Using a laptop to do Uni work in a public place	6. Inserting an unfamiliar DVD or USB into a Uni computer	7. Not reporting security incidents	Interviewee Organisation Date 5
1. Inconsiderate of other people's safety	2	1	4	3	3	4	5	Inconsiderate of own safety
2. Easier to identify as dangerous	1	2	3	3	4	4	5	Harder to identify as dangerous
3. More harmful to information	1	3	5	1	3	4	2	Less harmful to information
4. Larger impact on me	1	1	4	4	4	5	5	Larger impact on others
5. Unfamiliar environment	5	5	4	4	2	4	4	Familiar environment
6. More negligent	2	3	2	1	4	1	1	Less negligent
7. Harm felt by Uni	5	4	1	2	2	1	3	Harm felt by students
8. More likely to cause technology damage	2	2	1	3	1	4	5	More likely to cause physical damage
9.								
10. Overall, less risky	4	3	2	3	1	5	4	Overall, more risky

Figure 3.
A sample filled-in repertory grid interview sheet

- *Potency (P)*: If the construct refers to behaviours as being less risky-more risky, low impact-high impact, few affected-many affected, etc.
- *Activity (A)*: For all other types of construct that could not be coded as "E" or "P", including inappropriate constructs such as "knowledge of policy-unaware of policy".

There were 188 constructs in total, comprising 44 "E"s, 56 "P"s and 88 "A"s. Constructs categorised as "A" were not used in this study.

After this core categorisation process, each interviewee's construct ratings across the seven behaviours were converted to a score that represented their attitude towards these behaviours. This was calculated by multiplying the mean of all the ratings for his or her "E" constructs by the mean of all the ratings for his or her "P" constructs represented by:

$$Attitude = \frac{\sum_{i=1}^{n} E_i}{n} \times \frac{\sum_{i=1}^{m} P_i}{m}$$

Where:

E_i = ith construct categorised as "E";
n = number of E constructs in the grid;
P_i = ith construct categorised as "P"; and
m = number of P constructs in the grid (Osgood *et al.*, 1957).

5. Results

5.1 Study 1: online survey questionnaire

Table IV below shows the 23 participant scores for the attitude statements in the online questionnaire for each of the seven behaviours. A high score (maximum = 5) indicates that the participant thought that the behaviour was risky and harmful. This represents a favourable and good attitude. Conversely, a low score (minimum = 1) indicates that the participant thought the behaviour was not risky and quite harmless. This represents an unfavourable and poor attitude towards behaviours. As shown in Table IV below, participants thought password management was the most risky behaviour and internet use was the least risky.

5.2 Study 2: repertory grid technique (RGT) interviews

Table V below shows the calculated RGT interview scores for the 23 interviewees for each of the seven naïve and accidental behaviours. A high score (maximum = 25) indicates that the interviewee thought that the behaviour was risky and harmful. This represents a favourable and good attitude. Conversely, a low score (minimum = 1) indicates that the interviewee thought the behaviour was not risky and quite harmless. This represents an unfavourable and poor attitude towards behaviours. As shown in Table V below, both social networking site use and information handling were considered most risky by participants, whereas mobile computing was considered least risky.

	Attitude scores						
No.	PM	EM	IU	SNS	MC	IH	IR
1	4	4	2	4	4	4	4
2	5	5	5	4	4	5	5
3	5	5	1	5	4	4	4
4	5	4	4	4	3	4	4
5	5	4	3	5	5	5	4
6	5	4	4	4	5	3	2
7	5	5	4	5	4	4	4
8	5	5	4	5	5	4	4
9	5	4	4	4	4	4	4
10	4	4	4	4	4	5	4
11	5	5	3	5	5	5	4
12	4	2	4	4	2	2	2
13	4	5	2	3	3	4	4
14	5	5	5	5	5	5	5
15	5	5	4	5	5	5	4
16	4	4	4	5	4	4	5
17	5	4	3	5	5	3	3
18	5	5	3	5	5	4	4
19	5	4	3	4	4	4	4
20	5	5	5	5	3	5	3
21	5	2	2	5	3	4	4
22	5	5	4	4	5	4	3
23	4	4	2	5	4	4	4
Mean	4.74	4.30	3.43	4.52	4.13	4.13	3.83

Table IV.
Attitude scores using online questionnaire

5.3 Summary of results

Table VI below shows how the results of the two studies correlated for each of the seven behaviours, namely password management (PM), email use (EU), internet use (IU), social networking (SNS), mobile computing (MC), information handling (IH) and incident reporting (IR).

These results indicate that there were significant relationships between the participants' scores from the two studies for three of the seven behaviours. The strongest relationship was for the measure of internet use, which was highly correlated, with the Spearman correlation coefficient explaining approximately 36 per cent of the variance. The measures of mobile computing and email use were also quite consistent for the two studies. The correlation for mobile computing explained approximately 21 per cent of the variance, with 8 per cent explained for the measures of email use. The other four behaviours were not significantly correlated, suggesting these may be more complicated variables that should be studied in more detail.

6. Limitations

The sample size of 23 participants probably contributed to low levels of statistical significance that did not reach the traditional $p < 0.05$ levels. However, the strength of the relationships (rho) between the two sets of results was encouraging given a sample size of less than 30.

No.	Attitude scores PM	EM	IU	SNS	MC	IH	IR
1	13.3	10.7	8.0	16.0	6.7	14.0	11.0
2	2.0	12.0	14.7	16.0	2.7	14.0	9.3
3	25.0	18.0	7.5	8.8	13.5	25.0	14.0
4	15.8	10.5	16.0	12.0	3.0	6.8	18.0
5	13.5	17.5	15.0	15.0	14.0	20.0	15.0
6	7.0	7.5	18.0	14.0	7.0	11.3	12.0
7	2.0	17.3	8.7	21.7	2.0	13.3	25.0
8	7.0	7.5	11.3	13.0	9.0	14.0	7.5
9	18.3	16.7	21.7	20.0	12.0	20.0	12.0
10	9.0	9.6	25.0	18.0	4.2	9.6	6.8
11	10.0	12.5	7.5	22.5	2.0	12.0	18.0
12	6.8	6.0	22.5	18.0	2.6	17.5	14.6
13	7.5	17.5	3.0	8.0	4.0	10.5	10.5
14	15.0	13.0	15.0	12.0	18.3	16.7	11.7
15	15.0	15.0	8.8	10.5	3.0	16.0	7.5
16	7.5	9.3	11.7	10.0	6.7	13.0	13.0
17	10.0	16.5	9.3	13.3	7.0	10.0	5.3
18	12.0	12.0	9.0	25.0	8.0	20.0	13.0
19	4.0	25.0	12.0	3.0	6.0	20.0	3.0
20	3.0	3.8	22.5	15.8	4.5	12.0	8.8
21	5.0	5.0	17.0	8.1	6.0	10.5	14.0
22	4.7	8.6	13.3	14.7	7.1	11.0	12.2
23	3.7	7.3	8.0	5.8	4.0	4.0	6.7
Mean	9.96	12.42	12.96	14.12	6.94	14.11	11.62

Table V.
Attitude scores using repertory grid technique (RGT) interviews

InfoSec behaviour	Spearman correlation coefficient (rho)	Sig. (two-tailed)	Coefficient of determination (R^2) (%)
Password management	0.105	0.635	1.10
Email use	0.275	0.203	7.56
Internet use	0.597**	0.003	35.64
Social networking	−0.043	0.847	0.18
Mobile computing	0.454*	0.029	20.61
Information handling	0.101	0.645	1.02
Incident reporting	0.020	0.927	0.04

Notes: *Correlation is significant at the 0.05 level (two-tailed); **correlation is significant at the 0.05 level (two-tailed)

Table VI.
Spearman correlations

This research project involved university students as participants that are not representative of typical employees despite the fact that most of them had part-time jobs. Future research will need to involve a more representative cross-section of employed people.

7. Conclusions and future directions

The aim of this research was to compare two studies that assessed the attitudes of typical computer users toward naïve and accidental InfoSec behaviour. The first study

used a quantitative self-reporting online survey instrument and the second study used a set of RGT interviews.

This research highlights the complexities associated with measuring InfoSec attitudes. Although three of the seven behaviours were significantly correlated, the relationships between the other four behaviours were small. This may, in part, be due to the large variation between individuals. As shown in Tables IV and V, behaviours that were rated as most risky by some individuals were rated as least risky by others.

It is important to highlight that the methodologies of both studies have potential strengths and weaknesses. For example, although the self-reporting methodology may be criticised as it can be biased by social desirability, it is a quick and efficient method of obtaining a large amount of data from a large number of participants. In contrast, the RGT is a far more labour-intensive and time-consuming technique but has been shown to reduce socially desirable responses. When attempting to measure attitudes, perhaps a combination of the two techniques is most advisable.

This study contributes to the challenge of developing a reliable instrument that will assess individual InfoSec awareness (ISA). This assumes that such an instrument uses attitude as one of the contributing factors to ISA, such as the knowledge, attitude and reported behaviour (KAB) model (Parsons *et al.*, 2014). Senior management will be better placed to design intervention strategies, such as training and education of employees, if individual attitudes are known. This, in turn, will reduce risk-inclined behaviour and a more secure organisation.

References

Abraham, S. (2011), "Information security behaviour: factors and research directions", *AMCIS 2011 Proceedings – All Submissions Paper 462*, available at: http://aisel.aisnet.org/amcis2011_submissions/462.

Ajzen, I. (1991), "The theory of planned behaviour", *Organisational Behaviour and Human Decision Processes*, Vol. 50 No. 2.

Ajzen, I. and Fishbein, M. (1973), "'Attitudinal and normative variables as predictors of specific behaviour '", *Journal of Personality and Social Psychology*, Vol. 27 No. 1, pp. 41-57.

Ajzen, I. and Fishbein, M. (2000), "Attitudes and the attitude-behavior relation: reasoned and automatic processes", *European Review of Social Psychology*, Vol. 11 No. 1, pp. 1-33.

Armsby, P., Boyle, A. and Wright, C. (1989), "'Methods for assessing drivers' perception of specific hazards on the road", *Accident Analysis & Prevention*, Vol. 21 No. 1, pp. 45-60.

Bannister, D. (1981), "Personal construct theory and research method", *Human Inquiry: A Sourcebook of New Paradigm Research*, John Wiley & Sons, New York, NY.

Cassell, C. and Walsh, S. (2004), "Repertory Grids", in Cassell, C. and Syman, G. (Eds), *Essential Guide to Qualitative Methods in Organizational Research*, Sage Publications, London, pp. 61-72.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90-101.

Curtis, A., Wells, T., Lowry, P. and Higbee, T. (2008), "An overview and tutorial of the repertory grid technique in information systems research", *Communications of AIS*, Vol. 2008 No. 23, pp. 37-62.

Darley, J.M. and Latane, B. (1968), "Bystander intervention in emergencies: diffusion of responsibility", *Journal of Personality and Social Psychology*, Vol. 8 No. 4, p. 377.

Fishbein, M. and Ajzen, I. (1975), *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, Addison-Wiley Publishing Company, Massachusetts.

Fransella, F., Bell, R. and Bannister, D. (2004), *A Manual for Repertory Grid Technique*, 2nd ed., John Wiley & Sons, West Sussex.

Furnell, S., Jusoh, A. and Katsabas, D. (2006), "The challenges of understanding and using security: a survey of end-users", *Computers & Security*, Vol. 25 No. 1, pp. 27-35.

Hair, N., Rose, S. and Clark, M. (2009), "Using qualitative repertory grid techniques to explore perceptions of business-to-business online customer experience", *Journal of Customer Behaviour*, Vol. 8 No. 1, pp. 51-65.

Heise, D.R. (1970), "The semantic differential and attitude research", Chapter 14, *Attitude Measurement*, in Summers, G. (Ed.), Chicago, USA, pp. 235-253.

Jankowicz, D. (2004), *The Easy Guide to Repertory Grids*, John Wiley & Sons, West Sussex.

Kelly, G. (1955), *The Psychology of Personal Constructs*, Vols 1/2, Norton, New York, NY.

Kervyn, N., Fiske, S.T. and Yzerbyt, V.Y. (2013), "Integrating the stereotype content model (warmth and competence) and the Osgood semantic differential (evaluation, potency, and activity)", *European Journal of Social Psychology*, Vol. 43 No. 7, pp. 673-681.

Kruger, H. and Kearney, W. (2006), "A prototype for assessing information security awareness", *Computers & Security*, Vol. 25 No. 4, pp. 289-296.

Leach, J. (2003), "Improving user security behaviour", *Computers & Security*, Vol. 22 No. 8, pp. 685-692.

McGuire, W.J. (1969), "The nature of attitudes and attitude change", *The Handbook of Social Psychology*, Vol. 3 No. 2, pp. 136-314.

Myers, B., Hollan, J., Cruz, I., Bryson, S., Bulterman, D., Catarci, T., Citrin, W., Glinert, E., Grudin, J. and Ioannidis, Y. (1996), "Strategic directions in human-computer interaction", *ACM Computing Surveys (CSUR)*, Vol. 28 No. 4, pp. 794-809.

Olson, G. and Olson, J. (2003), "Human-computer interaction: psychological aspects of the human use of computing", *Annual Review of Psychology*, Vol. 54 No. 1, p. 491.

Osgood, C., Suci, G. and Tannenbaum, P. (1957), *The Measurement of Meaning*, University of Illinois Press, Urbana, Illinois, USA.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Computers & Security*, Vol. 42 No. 15, pp. 165-176.

Pattinson, M. and Anderson, G. (2007), "How well are information risks being communicated to your computer end-users?", *Information Management & Computer Security*, Vol. 15 No. 5, pp. 362-371.

Schneier, B. (2004), "The people paradigm", available at: www.csoonline.com/article/219787/bruce-schneier-the-people-paradigm (accessed 23 June 2011).

Schrader, P. and Lawless, K.A. (2004), "The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments", *Performance Improvement*, Vol. 43 No. 9, pp. 8-15.

Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security*, Vol. 24 No. 2, pp. 124-133.

Stewart, V., Stewart, A. and Fonda, N. (1981), *Business Applications of Repertory Grid*, McGraw-Hill Companies, London.

Tan, F. (1999), "Exploring Business-IT alignment using the repertory grid", in *Proceedings of the 10th Australasian Conference on Information Systems (ACIS)*, pp. 931-943.

Tan, F. and Hunter, M. (2002), "The repertory grid technique: a method for the study of cognition in information systems", *MIS Quarterly*, Vol. 26 No. 1, pp. 39-57.

Thomson, M. and von Solms, R. (1998), "Information security awareness: educating your users effectively", *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167-173.

Trček, D., Trobec, R., Pavešsić, N. and Tasič, J. (2007), "Information systems security and human behaviour", *Behaviour & Information Technology*, Vol. 26 No. 2, pp. 113-118.

Vroom, C. and von Solms, R. (2004), "Towards information security behavioural compliance", *Computers & Security*, Vol. 23 No. 3, pp. 191-198.

Whyte, G. and Bytheway, A. (1996), "Factors affecting information systems' success", *International Journal of Service Industry Management*, Vol. 7 No. 1, pp. 74-93.

Wilde, G.J. (1994), *Target Risk*, PDE Publications, Toronto.

Wilde, G.J. (1998), "Risk homeostasis theory: an overview", *Injury Prevention*, Vol. 4 No. 2, pp. 89-91.

Zhang, P., Benbasat, I., Carey, J., Davis, F., Galletta, D. and Strong, D. (2002), "Human-computer interaction research in the MIS discipline", *Communications of the AIS*, Vol. 9 No. 20, pp. 334-355.

Corresponding author
Malcolm Pattinson can be contacted at: malcolm.pattinson@adelaide.edu.au