Examining Attitudes toward Information Security Behaviour using Mixed Methods

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

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

Abstract

This paper reports on a mixed-method research project that examined the attitudes of computer users toward accidental/naive information security (InfoSec) behaviour. The aim of this research was to investigate the extent to which attitude data elicited from repertory grid technique (RGT) interviewees support their responses collected via an online survey questionnaire. Twenty five university students participated in this two-stage project. Individual attitude scores were calculated for each of the research methods and were compared across seven behavioural focus areas using Spearman product-moment correlation coefficient. The two sets of data exhibited a small-to-medium correlation when individual attitudes were analysed for each of the focus areas. In summary, this exploratory research indicated that the two research approaches were reasonably complementary and the RGT interview results tended to triangulate the attitude scores derived from the online survey questionnaire, particularly in regard to attitudes toward Incident Reporting behaviour, Email Use behaviour and Social Networking Site Use behaviour. The results also highlighted some attitude items in the online questionnaire that need to be reviewed for clarity, relevance and non-ambiguity.

Keywords

Information Security (InfoSec), InfoSec Behaviour, Repertory Grid Technique (RGT), Theory of Planned Behaviour, Attitude, Mixed Methods, Hybrid

1. Introduction

1.1. Background

There is a growing body of literature (Schneier 2004, Vroom and von Solms 2004, Stanton, Stam et al. 2005, Pattinson and Anderson 2007, Trček, Trobec et al. 2007) 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 instead of, addressing hardware and software solutions. This human 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 human behavioural solutions to achieve the purported benefits that a positive change in computer user behaviour can have on the security of their computer systems even though very little rigorous research has been conducted to-date to confirm this management practice. This is borne out by Abraham's (2011) "extensive literature review on information security behavior in the context of factors affecting security behavior (sic) of users in organizational environments" (p. 1). In this review she cites a paper by (Thomson and von Solms 1998) as one of a small number of studies that "recognized the effects of users' attitudes in shaping security behaviour" (p. 5).

The research described in this current paper focuses on behavioural information security. More specifically, it examines the attitudes that computer users have towards accidental/naïve behaviour. Examples of accidental/naïve 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 investigate the extent to which attitude data elicited from repertory grid technique (RGT) interviewees support their responses collected via an online survey questionnaire. In other words, is the online survey questionnaire, on its own, a reliable instrument for extracting the attitudes of computer users toward various types of accidental/naive InfoSec behaviour?

The objectives of this research were to:

- Develop and distribute an online survey questionnaire for University students to complete
- Analyse the data and calculate an attitude score for each participant for each type of behaviour
- Interview the same students using the semi-structured interviewing method known as the Repertory Grid Technique(RGT)
- Analyse the data and calculate an attitude score for each participant for each type of behaviour
- Compare the results and report on the extent to which the interview results supported the survey results.

The structure of this paper is as follows. The next section outlines the justification for this research and this is followed by a summary of the most relevant literature and the theories that underpin the research. The research methods deployed are then discussed. Finally the results are explained, findings are discussed and conclusions are presented.

2. Justification for this research

This paper reports on research that is motivated by the need to measure the attitudes of employees toward InfoSec behaviour so that intervention strategies can be implemented that will improve attitudes and mitigate 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.

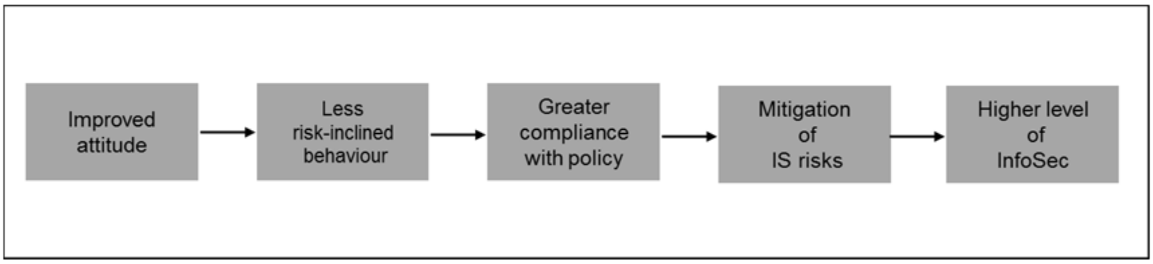


Figure 1: Logic hierarchy of this current research

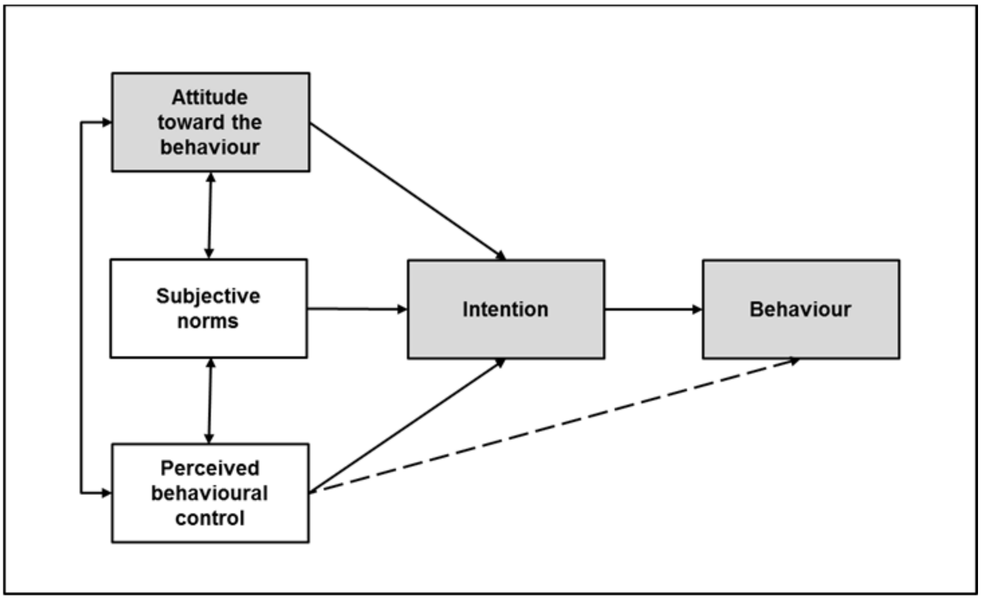
The Crossler, Johnston et al. (2013) paper titled *Future directions for behavioral information security research* highlights the need for research that addresses better methods of collecting, eliciting and measuring security-related data, particularly attitude data. Furthermore, this paper also calls for research that differentiates between insider deviant behaviour and insider misbehaviour. This current research contributes to both these requests by firstly, using a mixed-method research approach and secondly, by focusing on only accidental/naive behaviour.

3. Theoretical Issues & Literature

3.1. Overview

There is a considerable amount of research literature on the subject of general human behaviour (Ajzen and Fishbein 1973, Ajzen 1991, Brown 2005). Although there are numerous publications relating to the interaction between humans and computer systems, (commonly known as human-computer interaction (HCI)) (Myers, Hollan et al. 1996, Zhang, Benbasat et al. 2002, Olson and Olson 2003, Parsons, McCormac et al. 2014), there is very little rigorous research devoted to factors that may influence safe/unsafe user behaviour. It has only been in the last decade that literature has emerged out of the InfoSec discipline that discusses the impact of individual behaviour whilst using a computer (Leach 2003, Stanton, Stam et al. 2005, Trček, Trobec 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.



(shaded areas indicate the scope of this research)

Figure 2: Theory of Planned behaviour

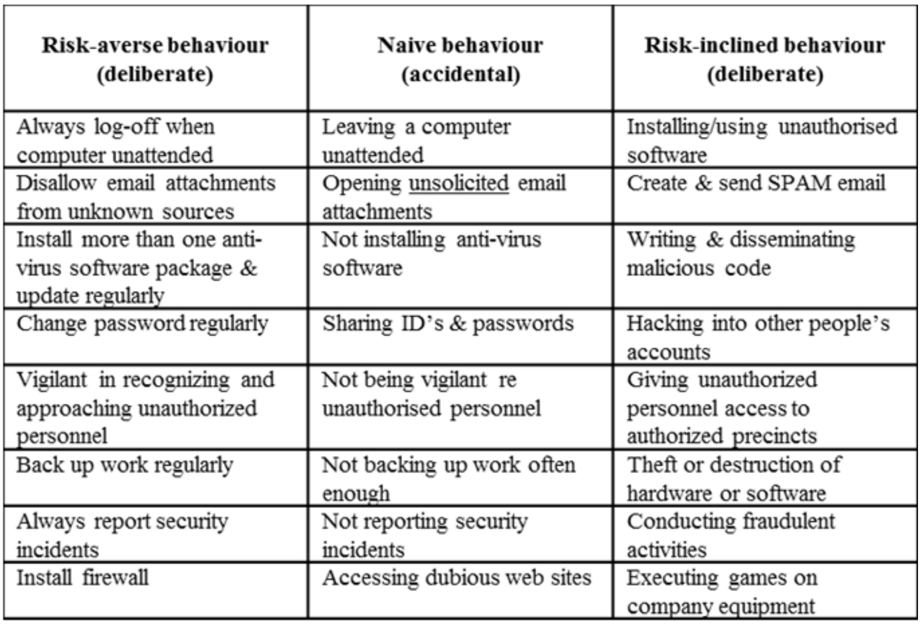
Many studies have been conducted since (Fishbein and Ajzen 1975) and (Ajzen 1991) developed the theories of reasoned action (TRA) and planned behaviour (TPB) in an attempt to understand peoples' intentions to engage in a variety of activities. These theories are based on the assumption that intentional behaviour is directly related to actual behaviour (Fishbein and Ajzen 1975).

3.2. Human Behaviour

The disciplines of economics and social psychology have generated a large amount of literature, research and knowledge relating to human behaviour within organisations. In these studies, numerous theories have been espoused, many phenomena have been analysed and reported on and many concepts and principles have been developed. Examples are the Risk Homeostasis theory (Wilde 1994, Wilde 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 accidental/naive behaviour that relates to the security of an organisation's information systems.

3.2.1. Information Security (InfoSec) behaviour

Information security behaviours have been categorised in different ways by numerous studies (Stanton, Stam et al. 2005, Pattinson and Anderson 2007, Parsons, McCormac et al. 2014). For example, Stanton, et al (2005) refer to risk-averse behaviours as 'Aware Assurance' or 'Basic Hygiene'; naive behaviours as 'Dangerous Tinkering' or 'Naïve Mistakes': and risk-inclined behaviours as 'Intentional Destruction' or 'Detrimental Misuse'. For the purposes of this research and this paper, the term "InfoSec behaviour" refers to the full spectrum of behaviours by people who make significant use of computers as part of their job. As shown in Table 1 below, these behaviours range from deliberate risk-averse behaviours to deliberate risk-inclined behaviours.



Risk-averse behaviour (deliberate)	**Naive behaviour (accidental)**	**Risk-inclined behaviour (deliberate)**
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 & send SPAM email
Install more than one anti-virus software package & update regularly	Not installing anti-virus software	Writing & disseminating malicious code
Change password regularly	Sharing ID’s & passwords	Hacking into other people’s accounts
Vigilant in recognizing and approaching unauthorized personnel	Not being vigilant re unauthorised personnel	Giving unauthorized personnel access to authorized 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 1: Examples of InfoSec behaviours (Pattinson and Anderson 2007)

The research described in this paper is focussed only on accidental/naive behaviours, examples of which are shown in the middle column of Table 1 above.

3.3. Attitude toward Behaviour

Although the concept of “attitude” is both complex and has been defined in many different ways by different researchers (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. This concept is universally understood as an overall feeling of a behaviour being favourable or unfavourable (Ajzen and Fishbein 2000). Other descriptions that are used include behaviour that is liked or dis-liked; desirable or un-desirable; good or bad; or behaviour that is viewed positively or negatively. This research project is concerned with information security behaviour, or more specifically, accidental/naïve behaviour of computer users. For the purposes of this paper, attitudes toward this type of behaviour are perceived as 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?

3.4. Repertory Grid Technique (RGT)

The RGT is a cognitive technique that was developed by, and is grounded in George Kelly’s Personal Construct Theory (1955). 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 wide variety of applications within different domains such as in psychology studies (Bannister 1981, Armsby, Boyle et al. 1989) and in management research (Tan 1999). In terms of relevance to this paper, 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” (pp. 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.

Any number of psychological tools and techniques could be adapted to study the impact that user attitude has on accidental/naïve behaviour. However, Kelly’s (1955) personal construct theory and the RGT appear to be ideally suited to the aims of this research and to the qualitative nature of the information being sought. 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, Bell 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, Wells et al. 2008).

4. Research Methods

4.1. Overview

The research approach described in this paper is a mixed-method (that is, hybrid) research approach (Johnson and Christensen 2008). This particular mixed-method research design is a two-stage sequential design which incorporates an initial quantitative stage (online questionnaire) followed by a hybrid qualitative/quantitative stage (RGT interviews). The main reason for using a mixed-method approach for this project was to develop a complementary picture and to compare and triangulate results (Plano Clark and Badiee 2010). Furthermore, the topic being examined is "attitudes", that is, what humans think or feel about something, and in this project, it is their attitude toward accidental/naive risky behaviour of computer users. Therefore, it was appropriate that a quantitative stage should be followed by a qualitative (well, hybrid really) stage.

Participants were university students who were recruited via email. Most of the students were less than 30 years of age and had part time jobs. There were approximately equal number of males and females spread across all levels of university courses.

4.2. Stage 1

In this Stage, 122 students undertook a web-based survey that was accessible within a specific computer laboratory on the University campus. This online Qualtrics survey consisted of demographic questions; computer usage questions; personality and cognitive questions; and knowledge, attitude and behaviour questions. Refer Parsons, McCormac et al. (2014) for a more detailed explanation of this survey. The survey took approximately 40 minutes to complete for which participants were paid $30.

Participants were asked to rate 21 statements relating to their attitude towards computer-based behaviour on a 5-point rating scale ranging from “Strongly disagree” to "Strongly agree". Three statements were posed for each of the seven focus areas, namely, Password Management (PM), Email Use (EM), Internet Use (IU), Social Networking Site Use (SNS), Mobile Computing (MC), Information Handling (IH) and Incident Reporting (IR).

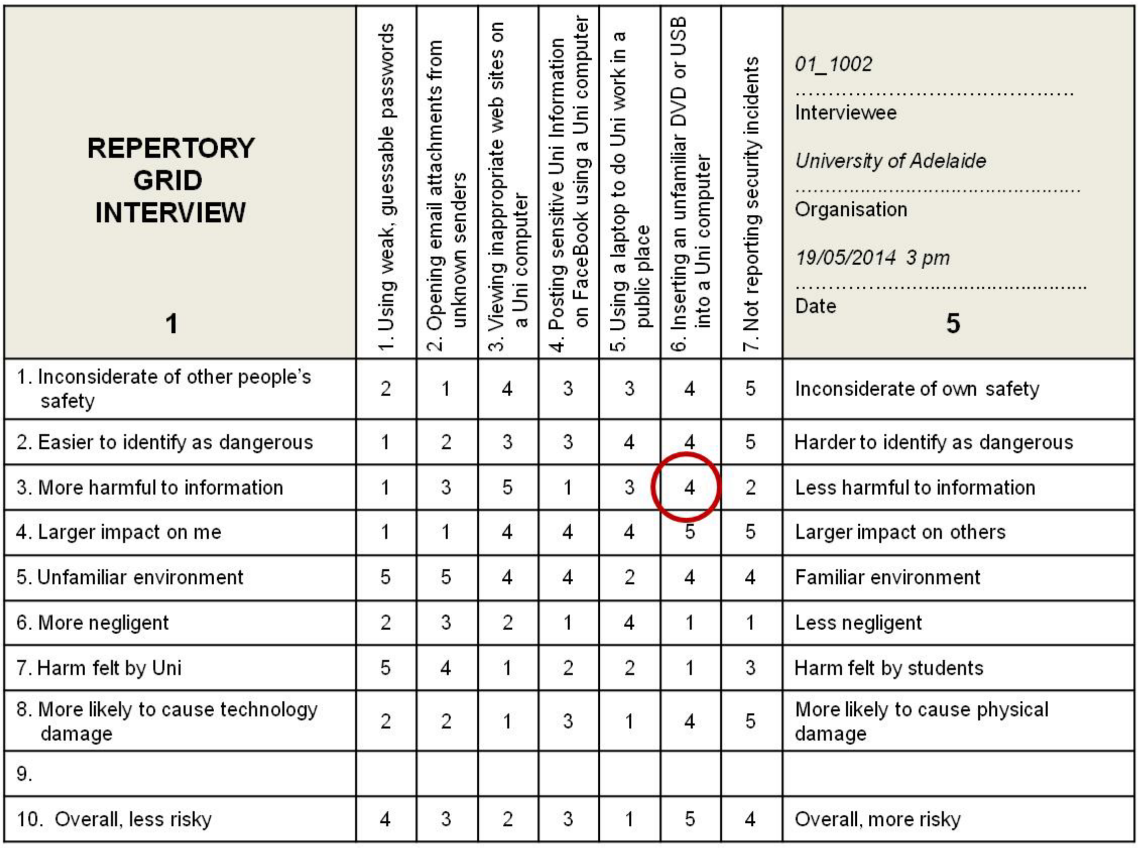
Approximately half of the statements were expressed in negative terms and questions were presented in random order of focus area. Each participant recorded 21 scores between 1 and 5. Negative questions were reversed prior to analysis. High scores represent a more favourable and better attitude toward InfoSec behaviours. Conversely, low scores represent an unfavourable and poor attitude. (Refer Table 2 in Section 5).

4.3. Stage 2

In this Stage, 25 participants from the pool of 122 who completed Stage 1, agreed to be interviewed by the researcher using the Repertory Grid Technique (RGT). The objective of these semi-structured interviews was to elicit the thoughts and views pertaining to their attitude toward information security (InfoSec) behaviours. Each interview took approximately 45 minutes and each participant was paid a further $30 for their involvement.

For these RGT interviews, a set of elements was required that represented this research's topic of interest, which was “*Attitudes toward information security behaviours*”. Although there are many approaches to developing such elements, it was decided to make these elements risk-inclined, accidental/naïve behaviours, using one from each of the seven focus areas used in Stage 1. 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 attitudes about InfoSec 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, Stewart et al. 1981). Interviewees were specifically asked “*What word or phrase would you use to describe the behaviour”.* On average, seven bi-polar constructs were generated 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 eight elicited bipolar constructs as rows (construct number 10 was supplied by the researcher). The 7 x 8 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, the interviewee of Figure 3 thought that behaviour number 6, "Inserting an unfamiliar DVD or USB into a Uni computer" was relatively "Less harmful to information" and scored it a "4" as shown circled in red.



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	*01_1002* Interviewee *University of Adelaide* Organisation *19/05/2014 3 pm* 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

The set of 25 repertory grids consisting of 204 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 (pp. 149). In order to analyse the raw grid data in a grounded theory manner, a set of themes (i.e. categories) needed to be developed (Cassell and Walsh 2004). There are numerous approaches to doing this, for example, one could use categories from the research literature. However, it was decided to use Osgood's (1957) three basic dimensions of responses to semantic differential constructs that have been used to "measure" attitude. The three dimensions, namely, Evaluation, Potency, and Activity (EPA) have been used in a variety of studies, in particular, studies about attitudes (Heise 1970, Kervyn, Fiske et al. 2013). In this current study, constructs were categorised as:

- EVALUATION (E): if the construct refers to behaviours as being good-bad, accidental-deliberate, sensible-foolish, responsible-careless etc.
- 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'.

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:

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

where E_i = i^{th} construct categorised as "E", n = number of E constructs in the grid, P_i = i^{th} construct categorised as "P", m = number of P constructs in the grid. Overall results were calculated as the mean of the focus area scores.

All constructs categorised as "A" were not used in this study.

5. Results

5.1. Stage 1

Table 2 below shows how five of the 25 participants scored the attitude questions in the online questionnaire between 1 and 5 for each of the seven focus areas. A high score (maximum = 5) indicates that the participant thought that the behaviour was bad and harmful. This represents a favourable and good attitude. Conversely, a low score (minimum = 1) indicates that the participant thought the behaviour was not so bad and quite harmless. This represents an unfavourable and poor attitude towards behaviours. The "overall" score for each individual is simply the mean of all focus area scores.

Participant Number	Participant ID	PM	EM	IU	SNS	MC	IH	IR	Overall
1	01-1002	5	5	1	4	1	5	1	3.14
2	01-1004	5	4	2	4	2	2	3	3.14
3	01-1005	5	3	1	4	3	2	1	2.71
4	01-1008	5	4	3	4	2	2	1	3.00
5	01-1009	4	4	3	4	2	4	2	3.29

Table 2: Sample Attitude Scores from Online Questionnaire

5.2. Stage 2

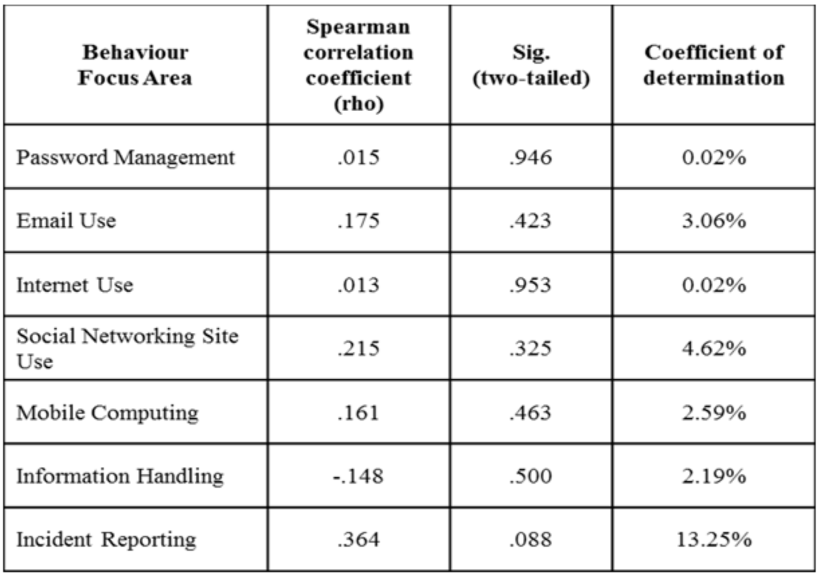
Table 3 below shows the calculated RGT interview scores for five of the 25 interviewees for each focus area. A high score (maximum = 25) indicates that the interviewee thought that the behaviour was bad and harmful. This represents a favourable and good attitude. Conversely, a low score (minimum = 1) indicates that the interviewee thought the behaviour was not so bad and quite harmless. This represents an unfavourable and poor attitude towards behaviours. The "overall" score for each interviewee is simply the mean of the focus area scores.

Interviewee Number	Interviewee ID	PM	EM	IU	SNS	MC	IH	IR	Overall
1	01-1002	12.0	10.0	9.0	18.0	8.8	12.3	10.5	11.50
2	01-1004	2.0	12.0	16.0	16.0	2.5	13.5	10.0	10.29
3	01-1005	25.0	18.0	7.5	10.0	15.0	25.0	14.0	16.36
4	01-1008	13.5	7.0	20.0	16.0	3.0	7.5	22.5	12.79
5	01-1009	15.0	10.0	5.0	10.0	16.0	15.0	5.0	10.86

Table 3: Sample Attitude Scores from Repertory Grid Technique (RGT) interviews

5.3. Summary of Results

The attitude scores for each of the two research methods were compared using Spearman product-moment correlation coefficient. The results for the individual attitudes toward each of the seven focus-area behaviours, showed small (rho > .10) to medium sized (rho > .30) correlations (Cohen 1988) between the two research methods, for most of the focus-area behaviours. This was achieved by comparing the individual scores for the seven attitude statements (items) in the questionnaire with the individual raw scores for each of the seven behaviours in the RGT interview (RGT elements).



Behaviour Focus Area	Spearman correlation coefficient (rho)	Sig. (two-tailed)	Coefficient of determination
Password Management	.015	.946	0.02%
Email Use	.175	.423	3.06%
Internet Use	.013	.953	0.02%
Social Networking Site Use	.215	.325	4.62%
Mobile Computing	.161	.463	2.59%
Information Handling	-.148	.500	2.19%
Incident Reporting	.364	.088	13.25%

Table 4: Spearman product-moment correlations

More specifically, the attitude of participants toward the behaviour of Reporting Security Incidents indicated a medium positive correlation between the survey questionnaire and the RGT interviews. For the other behaviours there was a small positive correlation between the two studies except for the behaviour Information Handling, which had a small negative correlation. Table 4 above also shows the coefficient of determination which indicates how much variance between the two studies that each of the seven attitudes share and although these percentages of variance are small, the results are encouraging and warrant further examination.

6. Limitations

1. The sample size of 25 participants was probably the reason that the levels of statistical significance (which suggest how much confidence one should have in the results), did not reach the traditional $p < .05$ levels. However, the strength of the relationships (rho) between the two sets of results was encouraging given the small sample size.

2. 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.

3. In retrospect, the design of the semi-structured RGT interviews could have been more aligned to the attitude statements in the survey questionnaire. Although they were similar, perhaps they needed to be identical.

4. The wording of some of the attitude statements in the survey questionnaire may have been ambiguous to participants. This observation has highlighted the need for constant updating to accommodate different populations, new behaviours and up-to-date hardware and software terminology.

7. Conclusions and future directions

The aim of this research was to investigate the extent to which attitude data elicited from repertory grid technique (RGT) interviewees support their responses collected via an online survey questionnaire. In other words, is the online survey questionnaire, on its own, a reliable instrument for extracting the attitudes of computer users toward various types of accidental/naive InfoSec behaviour?

In summary, the two research approaches were reasonably complementary and the RGT interview results tended to triangulate the attitude scores derived from the online survey questionnaire, particularly in regard to attitudes toward Incident Reporting behaviour, Email Use behaviour and Social Networking Site Use behaviour. The results also highlighted some attitude items in the online questionnaire that need to be reviewed for clarity, relevance and non-ambiguity.

This study contributes to the challenge of developing a reliable instrument that will assess individual InfoSec awareness (ISA) since attitude, (together with knowledge) is usually a principal component of ISA. 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 not only improve attitudes but will mitigate risk-inclined behaviour making for a more secure environment.

8. References

Abraham, S. (2011). Information Security Behaviour: Factors and research directions. AMCIS 2011 Proceedings - All Submissions. Paper 462.

Ajzen, I. (1991). "The theory of planned behaviour." Organisational Behaviour and Human Decision Processes **50**(2).

Ajzen, I. and M. Fishbein (1973). "Attitudinal and normative variables as predictors of specific behaviour " Journal of Personality and Social Psychology **27**(1): 41-57.

Ajzen, I. and M. Fishbein (2000). "Attitudes and the attitude-behavior relation: Reasoned and automatic processes." European review of social psychology **11**(1): 1-33.

Armsby, P., A. Boyle and C. Wright (1989). "Methods for assessing drivers' perception of specific hazards on the road." Accident Analysis & Prevention **21**(1): 45-60.

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

Brown, S. (2005). "Relationships between risk-taking behaviour and subsequent risk perceptions." British Journal of Psychology **96**(2): 155-164.

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

Cohen, J. W. (1988). Statistical power analysis for the behavioral sciences. Hillsdale, New Jersey, USA, Lawrence Erlbaum Associates.

Crossler, R. E., A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin and R. Baskerville (2013). "Future directions for behavioral information security research." Computers & Security **32**(0): 90-101.

Curtis, A., T. Wells, P. Lowry and T. Higbee (2008). "An Overview and Tutorial of the Repertory Grid Technique in Information Systems Research." Communications of AIS **2008**(23): 37-62.

Darley, J. M. and B. Latane (1968). "Bystander intervention in emergencies: diffusion of responsibility." Journal of personality and social psychology **8**(4p1): 377.

Fishbein, M. and I. Ajzen (1975). Belief, attitude, intention and behavior: An introduction to theory and research.

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

Hair, N., S. Rose and M. Clark (2009). "Using qualitative repertory grid techniques to explore perceptions of business-to-business online customer experience." Journal of Customer Behaviour **8**: 51-65.

Heise, D. R. (1970). "The semantic differential and attitude research." Attitude measurement: 235-253.

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

Johnson, B. and L. Christensen (2008). Educational research : quantitative, qualitative, and mixed approaches. Thousand Oaks, Calif., Sage Publications.

Kelly, G. (1955). The Psychology of Personal Constructs New York, Norton.

Kervyn, N., S. T. Fiske and V. Y. Yzerbyt (2013). "Integrating the stereotype content model (warmth and competence) and the Osgood semantic differential (evaluation, potency, and activity)." European Journal of Social Psychology **43**(7): 673-681.

Leach, J. (2003). "Improving user security behaviour." Computers & Security **22**(8): 685-692.

Myers, B., J. Hollan, I. Cruz, S. Bryson, D. Bulterman, T. Catarci, W. Citrin, E. Glinert, J. Grudin and Y. Ioannidis (1996). "Strategic directions in human-computer interaction." ACM Computing Surveys (CSUR) **28**(4): 794-809.

Olson, G. and J. Olson (2003). "Human-Computer Interaction: Psychological Aspects of the Human Use of Computing." Annual Review of Psychology **54**(1): 491.

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

Parsons, K., A. McCormac, M. Butavicius, M. Pattinson and C. Jerram (2014). "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)." Computers & Security **42**: 165-176.

Pattinson, M. and G. Anderson (2007). "How well are information risks being communicated to your computer end-users?" Information Management & Computer Security **15**(5): 362-371.

Plano Clark, V. L. and M. Badiee (2010). "Research questions in mixed methods research." Mixed Methods in Social and Behavioral Research: 275-304.

Schneier, B. (2004). "The People Paradigm." CSO Security and Risk Newsletter Retrieved June 23, 2011, from http://www.csoonline.com/article/219787/bruce-schneier-the-people-paradigm.

Schrader, P. and K. A. Lawless (2004). "The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments." Performance Improvement **43**(9): 8-15.

Stanton, J., K. Stam, P. Mastrangelo and J. Jolton (2005). "Analysis of end user security behaviors." Computers & Security **24**(2): 124-133.

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

Tan, F. (1999). Exploring Business-IT Alignment Using the Repertory Grid, Citeseer.

Tan, F. and M. Hunter (2002). "The Repertory Grid Technique: A Method for the Study of Cognition in Information Systems." MIS Quarterly **26**(1): 39-57.

Thomson, M. and R. von Solms (1998). "Information security awareness: educating your users effectively." Information Management & Computer Security **6**(4): 167-173.

Trček, D., R. Trobec, N. Pavešsić and J. Tasič (2007). "Information systems security and human behaviour." Behaviour & Information Technology **26**(2): 113-118.

Vroom, C. and R. von Solms (2004). "Towards information security behavioural compliance." Computers & Security **23**(3): 191-198.

Whyte, G. and A. Bytheway (1996). "Factors affecting information systems' success." International Journal of Service Industry Management **7**(1): 74-93.

Wilde, G. (1994). Target risk, PDE Publications Toronto.

Wilde, G. J. (1998). "Risk homeostasis theory: an overview." Injury Prevention **4**(2): 89-91.

Zhang, P., I. Benbasat, J. Carey, F. Davis, D. Galletta and D. Strong (2002). "Human-computer interaction research in the MIS discipline." Communications of the AIS **9**(20): 334-355.