Examining End-user Perceptions of Information Risks: An Application of the Repertory Grid Technique

M. R. Pattinson and C. Jerram

Business School, University of Adelaide, South Australia
e-mail: {malcolm.pattinson; cate.jerram}@adelaide.edu.au

Abstract

This paper proposes a research method that investigates the risk perceptions of computer end-users relating to organisational Information Security (InfoSec) and the situational factors that influence these perceptions. This method uses the Repertory Grid Technique (RGT) within recorded semi-structured interviews to elicit computer end-user perceptions, thoughts, beliefs and views pertaining to information security risks and threats. The suitability and appropriateness of using the RGT for this task is also discussed.

Keywords

Information Security (InfoSec), Information Risk, Risk Perception, Repertory Grid Technique (RGT), Psychometric Paradigm

1. Introduction

The need for adequate security of information systems has never been greater for organisations and individual computer users. Events that contribute to this need include:

- the increased use of, and dependence on the Internet for commercial transactions within public and private sectors
- the legal and statutory obligations of Chief Information Officers (CIOs) and Boards of Directors to comply with recent security standards and Information Security (InfoSec) legislation
- the added responsibility of Boards of Directors to establish effective governance of their organisation’s IT function
- the emergence and increased use of new technologies such as wireless, mobile commerce and social networking

This ever-increasing need has emphasised the importance that the security of information systems is maintained at a level acceptable to stakeholders. To achieve this goal, management have begun to realise that safeguards, controls, countermeasures and contingency plans must be put in place and diligently maintained. This business activity is commonly referred to as the management of InfoSec and is typically accomplished by installing hardware, implementing software, and developing effective policies and procedures.

There is a growing body of literature (Trcek et al, 2007; Schneier, 2004; Vroom et al, 2004; Stanton et al, 2005; Pattinson et al, 2007a, 2007b) that asserts that a more effective means of reducing information risk within an organisation is to address the behaviour of computer end-users in parallel with, and not instead of, hardware and software solutions. This human behavioural approach to managing InfoSec supports Schneier's (2004) claim that "...the biggest security vulnerability is still that link between keyboard and chair" (p. 1).

The research described in this paper focuses on human behavioural issues of computer end-users. More specifically, it examines the perceptions that computer end-users have of the risks and threats associated with their organisation's computer system and with the data that is stored and processed.

1.1. Aim of this Paper

The aim of this paper is to explain how the Repertory Grid Technique (RGT) can be incorporated into recorded semi-structured interviews to elicit end-user perceptions of information risk and to identify situational factors that contribute to these perceptions. This paper also discusses the pros and cons of the RGT for this intended purpose and argues that it is entirely appropriate for the collection of qualitative data such as perceptions, beliefs and views of computer end-users in regard to InfoSec.

2. Justification for Research

There is an abundance of literature available on how to manage InfoSec (Whitman et al, 2008; AS/NZS 27002:2006). Until about 2004, most of the solutions were very much based on the implementation of computer and telecommunications hardware and the application of software (Denning, 1999). Very little research was focussed on sociological and human behavioural solutions. Fortunately, a change in this focus is currently being witnessed, as researchers appreciate the importance of addressing human factors in their efforts to mitigate organisational information risks. Despite this trend, there is still a hiatus in rigorous empirical research relating to human factors within the InfoSec domain. This is borne out by the editors of MIS Quarterly, who express that:

"The literature in the area cries out for solid, theoretically grounded models and methods that will help ensure employee compliance. We (sic) especially challenge authors to not only adapt relevant theories from other fields, such as social psychology, but also to engage in IS security theory development to build models and methods for ensuring and explaining IS security policy compliance." (MISQ, 2007).

It is anticipated that the research alluded to in this paper will provide management with a basis for improving the risk perceptions of computer end-users by addressing the situational factors that are identified as having a significant impact on these perceptions. This, in turn, is predicted to have a positive effect on their behaviour whilst they are using a computer.

3. Literature Review and Terminology

3.1. Overview

There is a considerable amount of research literature on the subject of general human behaviour (Ajzen, 1991; Ajzen et al, 1973; Brown, 2005) and in particular, on the risk perceptions of individuals (Armsby et al, 1998; Bener, 2000; Fischhoff et al, 1993; Lapidus et al, 2006; Otway, 1980). This literature emanates mostly out of the disciplines of sociology, psychology, health, economics and education and relates to risk perceptions associated with activities such as investing in shares, driving motor cars, practicing safe sex and gambling. When it comes to the information systems domain, the story is somewhat different. Although there are numerous publications relating to the interaction between humans and computer systems, (commonly known as human-computer interaction (HCI)) (Myers et al, 1996; Olson et al, 2003; Zhang et al, 2002), there is very little evidence of research devoted to the behaviour of computer-end users. It has only been in the last four years that literature has emerged out of the InfoSec discipline that discusses the impact of individual behaviour whilst using a computer (Stanton et al, 2005; Leach, 2003; Trcek et al, 2007). More specifically, literature pertaining to the risk perceptions of computer end-users and the factors that may influence these perceptions is particularly scarce and represents a gap in InfoSec research.

3.2. Risks and Threats

There are numerous definitions of the terms ‘risk’ and ‘threat’ within many different contexts. In general terms though, a threat is any event, object or living entity that has the potential to put things of value at risk of being damaged, destroyed, lost, wounded, killed, corrupted or stolen. Risk, on the other hand, relates to the impact that might result if a threat occurs. In the domain of InfoSec, the ‘things of value’ are hardware, software, processes, people and most importantly, information. In the context of people’s perceptions in this domain, the terms ‘risk’ and ‘threat’ are often used synonymously. For example, when end-users are asked what they perceive as the risks to their organisation’s computer systems, they often say things like “virus attacks”, “unauthorised access” and “computer breakdowns”. These are not really risks, but threats. The risks caused by these threats are possibly loss of productivity; cost to recover the system; or information gets into the wrong hands. Because of this common mis-use of these terms, this paper uses the term ‘risks’ to mean ‘risks and threats’ and therefore assumes the term ‘risk perception’ to mean both the perception of risks and the perception of threats.

3.3. Risk Perception

There have been many studies over many decades that have examined how people perceive different threats or risks (or hazards as they are referred to in community environments). The earliest evidence of such research into risk perception was conducted by Starr in 1969 (Starr, 1969) but it seems that the real ‘founders’ of research into the factors that affect risk perceptions (of all sorts) were Fischhoff et al (1978), Slovic et al (1980) and Slovic (1987). They conducted the first psychometric studies that identified factors that influence perceptions of various hazards. Fischhoff's (1978) study investigated perceived risks and other issues related to 30 different activities or technologies. For example, they included alcoholic beverages, contraceptives, home appliances, motor vehicles, pesticides and many more.

When it comes to risk perceptions pertaining to information systems and InfoSec, the research literature is not as prevalent as it is for topics such as driving motor cars, contracting HIV/AIDS, flying aeroplanes and a multitude of other non-information technology activities. A critical assessment of InfoSec research between 1990 and 2004 was carried out by Siponen et al (2007) in which they found that research into the topic of risk management constituted only 2.96% of all InfoSec research (p. 1555). Research into the risk perceptions of computer end-users, a subset of information risk management, is even more scarce. Notwithstanding, three pieces of research are particularly relevant to this topic. The first of these is Lippa's (1994) research where he claims that an individual's perception of risks is shaped by the way in which risky situations are communicated to them within a particular organisational context. The second relevant study is Bener's (2000) thesis where she claims that the manner in which risk is communicated within an organisation substantially influences the risk perception of the different individuals within that organisation. And finally, research conducted by Huang, Rau and Salvendy (2007 and 2008) investigated the factors that can influence people's perception of different threats to information security.

3.4. Factors that Influence Risk Perception

There are an enormous number of factors that have been shown to influence people's perceptions of general threats, hazards or risks that relate to their health and well-being. A summary of the different types of factors, sourced from the literature, is shown below:

- personality characteristics such as a person's disposition, their propensity to take risks and their appetite for risk (Cooper, 2003);
- demographic variables such as gender, age, experience, and education (Bouyer et al, 2001);
- organisational factors such as job dissatisfaction, position within the organisation, how well the risks are communicated and organisational culture (Bener, 2000);
- sociological factors such as individual culture, social experiences, trust and beliefs (Jenkin, 2006);
- psychological factors such as risk sensitivity, attitude, and specific fear (Sjoberg, 2000) and
- properties of the risk such as expected loss or impact, beliefs about the cause and catastrophic potential (Jenkin, 2006).

This paper is only concerned with the last category of factors, namely, the properties of the risk, and refers to them as situational factors.

3.5. Repertory Grid Technique (RGT)

The RGT is a cognitive technique that was developed by, and is grounded in George Kelly's Personal Construct Theory (Kelly, 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); in management research (Tan, 1999) and for research into how drivers of motor cars perceive certain road hazards (Armsby et al, 1998). In terms of relevance to this paper, the RGT has also been applied in the information technology domain by Tan et al (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 conducted interviews with business people and elicited their perceptions about the level of success of the information systems they use.

Any number of psychological tools and techniques could be adapted to study the risk perceptions of computer end-users and the factors that contribute to these perceptions. 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 minimise or eliminate researcher bias and provide a high degree of transparency to interviewees (Curtis et al, 2008). They also claim that the RGT is advantageous compared to other elicitation techniques because it facilitates both qualitative and quantitative data analysis.

4. Method

4.1. Overview

The method proposed in this paper employs the RGT to examine the risk perceptions of computer end-users and to identify the situational factors that influence these perceptions. It is a four step process as follows:

1. Conduct semi-structured interviews with a theoretical sample of computer end-users to identify a list of risks that will become the elements in the final set of repertory grids.
2. Conduct semi-structured interviews with a theoretical sample of computer end-users to develop a number of psychometric scales that represent qualitative characteristics of the risks identified above. These will be the constructs in the final set of repertory grids.
3. Using the final set of repertory grids, get the theoretical sample of computer end-users to evaluate each of the risks on each of the bi-polar construct scales.

4. Conduct statistical analyses to identify a set of underlying factors that influence end-user perceptions of information risk.

The four steps are described in more detail below.

4.2. Step 1: Identify the Elements

This task involves the eliciting of grid elements, that is, perceived risks, via recorded semi-structured interviews with a theoretical sample of computer end-users who work within a variety of organisations and who use a computer for most of their job function. The number of interviews will depend on the point at which saturation is reached. That is, interviewing ceases when no new perceived risks are being raised.

Some previous applications of the RGT use grid elements pre-determined by the researcher, but this research recommends starting with a blank slate and letting the participants determine grid elements that relate to their personal circumstances and experiences. This alternative approach ensures that researcher bias is minimised and that the risks are topical and relevant.

The following list is a sample of the risks that were elicited in a pilot study exercise:

- Unauthorised access (internal)
- Unauthorised access (external)
- Virus brought in on USB and other media
- Reputation of firm damaged
- Information contamination
- Workstation malfunction
- Fraud
- Human error

It should be noted here that some of these perceptions were of risks but the majority were actually perceptions of threats. It became apparent that most end-users did not know the difference between a threat and a risk and so this paper assumes risk perceptions and threat perceptions to be synonymous (refer section 3.2).

The initial list of all elicited risks will be grouped into a manageable set of approximately 10 to 15 RGT elements as the basis for the next step.

4.3. Step 2: Develop Constructs

This task involves the eliciting of RGT constructs via recorded semi-structured interviews and is considered by many authors (Stewart et al, 1981; Armsby et al, 1998; Curtis et al, 2008) to be the most critical step of the RGT. Constructs are the ‘things’ that enable individuals to express their thoughts, beliefs or views about a particular object or event (Kelly, 1955). In this case, those ‘things’ are risks to an organisation’s information systems.

RGT constructs are ideally elicited from survey participants using the techniques of triading, laddering and pyramiding the grid elements. However, some applications of the RGT use pre-determined constructs like the nine bi-polar items of the psychometric paradigm (Fischhoff et al, 1978: Jenkin, 2006). The problem with this easier approach is that constructs sourced from the literature are not as meaningful to the population being surveyed (Armsby et al, 1998). Also, the reported benefits of the RGT would not be fully realised if constructs were simply 'manufactured' rather than elicited. Consequently, the research proposed in this paper will use constructs elicited from the survey participants by focussing on the qualitative properties of the RGT elements, in this case the information risks. To achieve this, the interviews will be structured in such a way as to encourage participants to think about each of the risks in terms of the following characteristics or properties:

- The likelihood of occurring
- How it could occur
- The damage caused
- What you stand to lose
- The cost to recover
- The impact to you and your productivity
- How to control it
- The perpetrators

It is expected that these interviews will elicit many different constructs relating to the above properties of the risks. These will need to be categorised into a manageable set of approximately 10 to 15 bi-polar constructs.

4.4. Step 3: Evaluate the Risks

Table 1 below shows a set of nine likely bi-polar constructs, each with a 5-point scale, that is used for all RGT elements (that is, risks). Each participant will be asked to evaluate each of the 10 to 15 risks against each of the 10 to 15 bi-polar constructs by marking a number between 1 and 5. The shaded boxes indicate a single participant's evaluation of a particular risk.

Cannot use the computer	1	[✓ 2]	3	4	5	Computer fully functional
All my own fault	1	2	[✓ 3]	4	5	Somebody else's fault
Large cost to recover from	1	2	3	[✓ 4]	5	Minimal recovery costs
Unknown damage	1	[✓ 2]	3	4	5	Obvious damage
Immediate impact	1	2	3	4	[✓ 5]	No impact felt
Rarely occurs	1	2	[✓ 3]	4	5	Occurs quite often
Difficult to prevent	1	2	3	[✓ 4]	5	Easy to prevent
Need to recover data	1	2	[✓ 3]	4	5	Data intact & accessible
A malicious act	[✓ 1]	2	3	4	5	An accidental mistake

Table 1: Sample Repertory Grid for all elements

4.5. Step 4: Analyse Data

The objective of this proposed research method is to identify a set of underlying situational factors that influence the risk perceptions of computer end-users. A variety of multivariate statistical methods could be used to achieve this. For example, Stewart et al (1981) promote the five principal methods of data analysis when using the RGT, namely, frequency counts, content analysis, visual focussing, cluster analysis and principal components analysis. However, the major objective of this data analysis is to determine the inter-correlations between the constructs and to group the constructs accordingly and label each group as a situational factor. This approach has been used by a number of researchers to date. For example, Fishhoff et al (1978) used the psychometric paradigm and its nine dimensions of risk to evaluate the risk perception of various community activities and technologies. They reduced the nine dimensions down to 2 factors, namely ‘technological risk’ and ‘severity’. A similar study by Slovic et al (1980) employed a factor analysis of 90 items to reveal three factors that influenced risk perceptions of general hazards. These were ‘dread’, ‘familiarity’ and ‘number of people exposed’. And finally, Huang, Rau and Salvendy (2007, 2008) conducted a factor analysis on 20 constructs from which they derived 6 factors, namely, ‘knowledge’, ‘impact’, ‘severity’, ‘controllability’, ‘possibility’ and ‘awareness’. This factor analysis approach has become an accepted approach in determining what factors influence risk perceptions (Huang et al, 2007; Siegrist et al, 2005) and therefore will be used in this proposed research method.

5. Conclusion

The aim of this paper is to explain how the RGT can be incorporated into recorded semi-structured interviews to elicit end-user perceptions of information risk and to identify situational factors that contribute to these perceptions. This paper also discusses the pros and cons of the RGT for this intended purpose and argues that it is entirely appropriate for the collection of qualitative data such as perceptions of information risk by computer end-users. Compared to many other techniques, the RGT appears to be a preferable approach because it facilitates both qualitative and quantitative data analysis (Curtis et al, 2008). It is a particularly beneficial approach when the research involves sensitive information, as is the case in this research. Previous studies (Kotulic et al, 2004) have reported that this type of information has not only been difficult to elicit, but has proved unreliable due to participants’ fear of retribution if they divulge sensitive details about their organisation.

6. References

Ajzen, I., 1991, “The theory of planned behavior”, Organizational Behavior and Human Decision Processes, Vol 50, Iss. 2.

Ajzen, I. and Fishbein, M., 1973, “Attitudinal and normative variables as predictors of specific behaviour”, Journal of Personality and Social Psychology, Vol. 27, Iss. 1, pp. 41-57.

Armsby, P., Boyle, A. J. and Wright, C. C., 1998, “Methods for Assessing Driver’s Perception of Specific Hazards on the Road”, Accident and Analysis Prevention, Vol. 21, No. 1, Pergamon Press, pp. 45-60.

AS/NZS 27002:2006, Information Technology - Security Techniques - Code of Practice for Information Security Management, Standards Australia/Standards New Zealand.

Bannister, D., 1981, "Personal Construct Theory and Research Method", in P. Reason and J. Rowan (eds.), Human Inquiry: A Sourcebook of New Paradigm Research, John Wiley and Sons Ltd, New York, USA.

Bener, A. B., 2000, "Risk Perception, Trust and Credibility: A Case in Internet Banking", PhD thesis, London School of Economics and Political Sciences, Available at http://is.lse.ac.uk/research/theses/default.htm, viewed 27 April 2005.

Bouyer, M., Bagdassarian, S., Chaabanne, S. and Mullet, E., 2001, "Personality Correlates of Risk Perception", Risk Analysis, Vol. 21, No. 3, pp. 457-465.

Brown, S. L., 2005, "Relationships between risk-taking behaviour and subsequent risk perceptions", British Journal of Psychology, Vol. 96, pp. 155-164.

Cooper, D., 2003, "Psychology, Risk and Safety – Understanding how personality and perception can influence risk taking", Professional Safety, November, www.asse.org.

Curtis, A. M., Wells, T. M. and Lowry, P. B., 2008, "An Overview and Tutorial of the Repertory Grid Technique in Information Systems Research", Communication of the Association for Information Systems, Volume 23, Article 3, pp. 37-62.

Denning, D. E., 1999, Information Warfare and Security, Addison Wesley, New York.

Fischhoff, B., Bostrom, A. and Quadrel, M. J., 1993, "Risk Perception and Communication", Annual Review of Public Health, Vol. 14, pp. 183-203.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. and Combs, B., 1978, "How Safe Is Safe Enough? A Psychometric Study of Attitudes towards Technological Risks and Benefits", Policy Sciences, Vol. 9, No. 2, pp. 127-152.

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.

Jenkin, C. M., 2006, "Risk Perception and Terrorism: Applying the Psychometric Paradigm", Homeland Security Affairs, Vol. II, No. 2, pp. 1–14.

Kelly, G.A., 1955, The Psychology of Personal Constructs, W.W. Norton and Company Inc., New York, USA.

Lapidus, J. A., Bertolli, J., McGowan, K. and Sullivan, P., 2006, "HIV–related risk behaviors, perceptions of risk, HIV testing, and exposure to prevention messages and methods among urban American indians and Alaska natives", AIDS Education and Prevention, The Guilford Press, 18(6), 546–559.

Leach, J., 2003, "Improving user security behaviour", Computers and Security, Vol. 22, p. 685-692.

Lippa, R. A., 1994, Introduction to Social Psychology, Second Edition, Wadsworth (Belmont, CA).

MISQ, 2007, Call for Papers, “MISQ Special Issue on Information Systems Security in a Digital Economy”, Available at: http://www.misq.org/BulletinBoard/ISSecurity.pdf, viewed 7 March 2008.

Myers, B., Hollan, J. and Cruz, I., 1996, “Strategic directions in Human–Computer Interaction”, ACM Computing Surveys, 28(4), 794 – 809.

Olson, G. M. and Olson, J. S., 2003, “Human–Computer Interaction: psychological aspects of the human use of computing”, Annual Review of Psychology, 54(1), 491 – 516.

Otway, H. J., 1980, “Risk Perception: A Psychological Perspective”, in M. Dierkes, S. Edwards and R. Coppock, (Eds.), Technological Risk: Its Perspective and Handling in Europe.

Pattinson, M. R. and Anderson, G., 2007a, “End-user Risk-taking Behaviour: An application of the IMB model”, Proceedings of 6th Annual Security Conference, Las Vegas, Nevada, USA, April.

Pattinson, M. R. and Anderson, G., 2007b, “How Well Are Information Risks Being Communicated To Your Computer End-Users?” Proceedings of International Conference on Human Aspects of Information Security and Assurance, Plymouth, England, July 10-12.

Schneier, B., 2004, “The People Paradigm”, http://www.csoonline.com/read/110104/counsel.htm, viewed 20/01/2006.

Siponen, M. and Willison, R., 2007, “A Critical Assessment of IS Security Research between 1990-2004.”, Proceedings of the 15th European Conference of Information Systems, St. Gallen, Switzerland, June 7-9, pp. 1551-1559.

Sjöberg, L., 2000, “Factors in Risk Perception”, Risk Analysis, Vol 20, No. 1, pp. 1-11.

Slovic, P., Fischhoff, B. and Lichtenstein, S., 1980, “Facts and Fears: Understanding Perceived Risk”, Societal Risk Assessment: How safe is Safe Enough?, Schwing, R. and Albers, Jr., eds., Plenum, New York, pp. 181-216.

Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J., 2005, “Analysis of end user security behaviour”, Computers and Security, Vol. 24, p. 124-133.

Stewart, V. and Stewart, A., 1981, Business Applications of Repertory Grid, London, 1981.

Tan, F. B., 1999, “Exploring Business-IT Alignment Using the Repertory Grid”, Proceedings of the 10th Australasian Conference on Information Systems.

Tan, F. B. and Hunter, M. G., 2002, “The Repertory Grid Technique: A Method for the Study of Cognition in Information Systems”, MIS Quarterly, Vol. 26, No. 1 pp. 39-57.

Trcek, D., Trobec, R., Pavesic, N. and Tasic, J.F., 2007, “Information systems security and human behaviour”, Behaviour and Information Technology, Vol. 26, No. 2, pp. 113-118.

Vroom, C. and Von Solms, R., 2004, “Towards information security behavioural compliance”, Computers and Security, Vol. 23, p. 191-198.

Whitman, M. E. and Mattord, H. J. 2008, Management of Information Security, 2nd edition, Thomson Course Technology.

Whyte, G. and Bytheway, A. 1996, “Factors affecting information systems’ success”, International Journal of Service Industry Management, Vol. 7, No. 1, pp. 74-93, MCB University Press.

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 Association for Information Systems, 9(20), 334 – 355.