2013

A Study of Information System Risk Perceptions at a Local Government Organisation

Malcolm Pattinson
The Univesity of Adelaide, Malcolm.Pattinson@adelaide.edu.au

Cate Jerram
The University of Adelaide, cate.jerram@adelaide.edu.au

Information Systems: Transforming the Future

24th Australasian Conference on Information Systems, 4-6 December 2013, Melbourne

Proudly sponsored by

ACIS 2013 Principal Sponsor

A Study of Information Systems Risk Perceptions at a Local Government Organisation

Malcolm Pattinson
Business School
University of Adelaide
South Australia
Email: malcolm.pattinson@adelaide.edu.au

Cate Jerram
Business School
University of Adelaide
South Australia
Email: cate.jerram@adelaide.edu.au

Abstract

This paper reports on a study that examined the perceptions of computer users in regard to the risks to their organisation's information systems (IS). A total of 12 employees from a local government organisation were interviewed in accordance with the Repertory Grid Technique (RGT). These structured interviews elicited a total of 110 constructs which represented individual thoughts, beliefs and views pertaining to information security (InfoSec) risks. These constructs were hermeneutically allocated into 28 categories of risk perception and then analysed via Content Analysis and Principal Component Analysis (PCA) to identify perceptions of IS risks and to uncover the major situational factors that influence these perceptions. The findings indicate that the local government participants perceived that the most serious risk to their organisation's IS was that systems will become unusable or unavailable such that large costs would be incurred to restore services and to maintain productivity. The situational factor that had the most influence on this IS risk perception was the type of loss suffered.

Keywords

Information Systems (IS), Information Security (InfoSec), Risk Perception, Repertory Grid Technique (RGT), Principal Component Analysis (PCA)

INTRODUCTION

The need for adequate security of information systems (IS) has never been more critical to the competitiveness and survival of organisations. Therefore, it is vital that an organisation's computing facilities are safeguarded and secured against a myriad of threats to the confidentiality, integrity and availability of the data that is processed.

Traditionally, management has relied heavily on hardware and software controls to mitigate the risks to their organisation's IS. However, many of these risks can be attributed to the behaviour of computer users and require socio-psychological and/or behavioural solutions to be implemented in tandem with hardware and software solutions.

The research outlined in this paper contributes to the ongoing quest for better information security (InfoSec) by examining how computer users perceive the risks to their organisation's IS.

Aim of this Research

The aim of this research was to examine how computer users perceive the risks to their organisation's IS. More specifically, this study identified the risks that were perceived by local government employees and also identified any underlying situational factors that had a major impact on these IS risk perceptions. Situational factors in this context are also referred to as "properties of the risk" and include such properties as expected loss, beliefs about the cause of the risk, frequency of occurrence of a particular security breach, severity of the impact and nature of the perpetrators (Jenkin 2006).

LITERATURE REVIEW

The perceptions that people have of the risks in everyday life have been shown by various socio-psychological studies to have a significant influence on individual decision-making and behaviour (Essau 2004 ; Jenkin 2006 ; Williams and Noyes 2007). For example, women who have a better perception of the risk of breast cancer are more likely to pursue mammography tests (Katapodi, Lee, Facione and Dodd 2004); and American Indians and urban natives who have a better perception of the risks of contracting HIV/AIDS are more likely to undertake HIV testing (Lapidus, Bertolli, McGowan and Sullivan 2006). This phenomenon also prevails in the domain of road safety where research has shown that drivers behave better (i.e. drive more safely) if they have a better perception of the risks (i.e. hazards) (Brown 2005 ; Machin and Sankey 2008). In summary, numerous studies in various domains have shown that people's behaviour becomes more risk-averse (and therefore less risk-inclined) as their perceptions of associated risks develop.

Accordingly, if this demonstrated positive relationship between perceptions of generic risk and subsequent behaviour, is applied to the domain of Information Technology (IT) it implies that better IS risk perceptions by computer users will translate into more responsible behaviour when they are working at a computer. For example, the Johnston and Warkentin (2010) investigation into the influence of fear appeals on behavioural intentions found that the perceptions that computer users have of the risks to themselves impacts on their decision-making and their subsequent behavioural intentions. Similarly, Lee and Larsen (2009) found that perceived severity (a major component of perceived risk) positively influences the behaviour of executives in small and medium businesses. They claim that "…the more seriously a person perceives the magnitude of the negative consequences ....the more he adopts recommended adaptive actions" (p. 180).

Does improved behaviour by computer users lead to greater compliance with InfoSec policies, which in turn, mitigates the risks to the organisation thereby providing a more secure IS environment?

The answer to this question is supported by numerous studies that examined the impact of computer-user behaviour on the state of InfoSec within organisations. For example, the study by Magklaras and Furnell (2005), which examined the various classifications of internal end-user sophistication, was based on the premise that the mis-use of computers by internal users is a major threat to the security of an organisation's IS. Similarly, the study by Stanton, Stam, Mastrangelo and Jolton (2005), which investigated what motivated computer users to behave the way that they do, was predicated on the assumption that better behaviour would reduce the risks to organisational IS. Pahnila, Siponen and Mahmood (2007) also support the argument that employee behaviour has a major influence on IS security. They claim that "Careless employees are a key threat to IS security" (p. 8). Finally, Vroom and von Solms (2004) who explored the potential problems of auditing user behaviour, claim that "The role of the employees is vital to the success of any company, yet unfortunately they are also the weakest link when it comes to information security [InfoSec]" (p. 3).

The research study described in this paper is predicated on the hypothesis that improved IS risk perceptions of computer users will translate into better organisational InfoSec.

RESEARCH METHOD

Background

This study involves the conduct of structured interviews that incorporate the Repertory Grid Technique (RGT) to elicit personal constructs from local government employees who use computers at their place of work. These constructs are conceptualised as perceptions of the risks to their organisation's computer systems and the data that these systems process. However, before constructs can be elicited, the technique requires that a set of "elements" be developed. These elements are objects, people, events or things about which the interviewee is familiar and is therefore likely to have thoughts, opinions or views - referred to by Kelly (1955) as constructs. After a series of prior interviews with typical computer users it was established, in accordance with a grounded theory approach, that a set of carefully-worded threats would be the best choice of RGT elements for this study. Consequently it was decided to use the following set of nine threats that were the most popular and understood, as the developed elements for each and every RGT interview:

- Hardware or network breakdowns
- Accidental data entry errors
- Being hacked by external persons
- Theft of hardware or media
- Virus attacks

- Flood, fire and other natural disasters
- Deliberate human errors, sabotage or vandalism
- Malware attacks like email spam, phishing, etc.
- Technical software failures (e.g. bugs).

Repertory Grid Technique (RGT)

The RGT is a cognitive method of interviewing in which interviewees divulge their attitudes, thoughts, perceptions and views about a particular situation, object or event. It is considered to be a hybrid, qualitative-quantitative approach to data collection and analysis (Tomico, Karapanos, Lévy, Mizutani and Yamanaka 2009). The qualitative aspects relate to the processes of eliciting constructs and rating these constructs for each RGT element during a one-on-one interview. The techniques of analysing the matrix of rating scores include both qualitative and quantitative methods. Jankowicz (2004) describes the RGT as "…a form of structured interviewing, with ratings or without, which arrives at a precise description uncontaminated by the interviewer's own viewpoint" (p. 14).

Essentially, the RGT enables researchers to discover how interviewees make sense of a specific "world", that is, how they personally construe particular situations based on their personal experiences. Originally, Kelly (1955) developed the technique for the purposes of exploring how individuals made sense of their social worlds. However, since that beginning, the use of the RGT has been expanded beyond sociological applications into a wide range of different environments within a variety of disciplines, including the IT/IS domain. For example, the RGT has been used to:

- analyse factors that effected the success of IS (Whyte and Bytheway 1996);
- identify "situational factors" that managers of IS development projects take into account when planning new projects (Moynihan 1996);
- investigate the personal constructs that users and IS professionals use to interpret information technology and its role in organisations (Tan and Hunter 2002);
- examine the cognitive basis of shared understanding between business and IS executives (Tan and Gallupe 2006);
- examine the skills that are deemed necessary to be a good IT project manager (Napier, Keil and Tan 2009);
- evaluate the design of web sites (Tan and Tung 2003);
- understand the important characteristics of good team members in software development projects (Siau, Tan and Sheng 2010).

Notwithstanding this wide-ranging deployment of the RGT within the IT/IS domain, there is no evidence of it being used to assess the security of IT/IS. This situation is indirectly supported by Curtis, Wells, Lowry and Higbee (2008), who, in their review of the use of the RGT in the IS domain, do not refer to any research related to InfoSec. Between 2008 and the time of writing this paper, there is similarly no evidence that the RGT has been used for research that evaluates the security of organisational IS.

One of the key reasons that the RGT was selected for this study was because the topic is considered by many people to be a sensitive issue and therefore subject to socially desirable participant responses. This research relates to the attitudes, thoughts and perceptions that interviewees have towards the security of their organisation's IS. Any research that delves into an employee's feelings about his employer creates a degree of unease, fear and nervousness within many employees at the thought that their job may be at stake if their responses are made known to their employer. This situation is made worse by the fact that this study is about risks to organisational computer systems and data. Questions such as "What am I supposed to think?" or "What answers should I give that will please my supervisor?" often arise in the minds of research interviewees. Although the RGT cannot totally eliminate socially desirable responses, at least the intrinsic techniques of triading, laddering and pyramiding will be as effective as any other social research method in keeping this type of response to a minimum (Jankowicz 2004).

Structured RGT Interviews

A series of 12 structured RGT interviews were conducted with employees from a large local government organisation. These interviews generated 110 rated bipolar constructs, which included for each of the 12

interviews, the supplied overall construct, "*Overall, less risky ----- Overall, more risky"*. This overall construct was supplied by the researcher and related to the perceived riskiness of each of the nine threats that were developed from prior interviews with typical computer users. This study averaged approximately nine constructs per grid which is consistent with previous studies that used the RGT (Reger 1990 ; Siau et al 2010 ; Tan et al 2002).

Each interview was recorded, not necessarily for transcription reasons, but in case there was a need to clarify some aspect of the interview at a later time. The interviewer used a common RGT interview form (as shown in Figure 1 below) to record interviewee responses.

REPERTORY GRID INTERVIEW 1	1. Hardware or network breakdowns	2. Accidental data entry errors	3. Being hacked by external persons	4. Theft of hardware or media	5. Virus attacks	6. Flood, fire & other natural disasters	7. Deliberate human errors, sabotage or vandalism	8. Malware attacks like email spam, phishing, etc	9. Technical software failures (e.g. Bugs)				Interviewee: xxxxxxxx Organisation: xxxxxxxx Date: xxxxxxxx 5
Has impact on information/data	4	2	1	4	2	3	1	4	3				Data intact to a known point
Negative impact on data retrieval	5	2	1	4	1	4	1	3	2				Retrieval of data can follow a process
Requires more analysis of the situation (don't know impact)	4	2	1	5	4	5	1	3	2				Requires less analysis of the situation (do know impact)
Don't know what's happened	5	3	2	4	2	5	2	3	4				Do know what's happened
I will be totally involved (more of a DR impact)	2	4	2	1	2	1	3	2	2				I will be somewhat involved
Requires in-house resolution	3	4	2	2	2	3	4	4	5				Means working with Vendor to solve
Potential for sensitive information to be leaked	5	2	1	1	1	5	1	4	5				No leakage of sensitive information
High financial impact	4	2	2	4	2	4	2	4	4				Usually only annoyance issue
Organisation's image at risk of being damaged	5	4	1	3	4	2	2	4	4				No impact on organisation's image
High media attention	5	5	2	3	3	1	1	4	4				Low media attention
Overall, less risky	2	2	4	2	4	4	4	2	2				**Overall, more risky**
Triads: 123, 456, 789, 147, 258, 369, 157, 268, 349													

Figure 1: RGT Interview Form

The RGT interview forms were designed specifically for this project and show the nine previously-developed elements. Interviewees were subjected to a traditional RGT interview after an explanation of the background to this research and reassurance about anonymity and confidentiality. The process involved using a set of nine index cards. On each card, one of the nine previously-developed RGT elements was written. These nine cards were placed in front of the interviewee and it was explained that the objective of the interview was to elicit their

thoughts (i.e. their constructs) regarding the risks posed by each of the nine threats to their organisation, to themselves or to other stakeholders, in the event that the specific threats actually occur.

Categorisation of Constructs

As part of the data analysis process a qualitative categorisation process was undertaken to reduce the 110 elicited constructs (minus the 12 supplied overall constructs) into a more manageable set of IS risk perception categories. This was done in accordance with the Jankowicz (2004) "bootstrapping" core categorisation process by using a variant of the hermeneutic circle (Gill 1994) in collaboration with independent experts. This method was preferred to many other valid approaches for developing themes or categories. For example, pre-existing categories may exist in literature such as text books, white papers, organisational policies and of course, research papers. Another source of valid and suitable categories can be found in relevant international Standards. In the case of this study, categories of IS risk perceptions were required, but they did not exist in the extant literature. Table 1 below shows the 28 categories within five themes that were created from the interview data.

Table 1: Categorised Constructs

	CATEGORIES WITHIN THEMES	No. of Constructs
1	**RISK PERCEPTIONS REALATING TO MY ORGANISATION**	
1.01	Reputation, credibility or image damaged	5
1.02	Quality/Integrity of data reduced	3
1.03	Increases costs/requires additional resources	8
1.04	Data is lost/destroyed/unrecoverable	5
1.05	Information gets into wrong hands/leaked	1
1.06	Systems down/unable to access information/reduced productivity	10
1.07	Customers/Sponsors lost	0
1.08	Hardware damaged or lost	1
1.09	Business can't operate or goes out of business	5
	Sub-total	**38**
2	**RISK PERCEPTIONS RELATING TO ME**	
2.01	I am reprimanded/demoted/fired	0
2.02	My personal information is damaged, destroyed or leaked	2
2.03	I can't do my job properly	8
2.04	Inconvenient/time-consuming/nuisance	2
2.05	My professionalism/quality of my work is tarnished	2
2.06	Causes me stress, anger, embarrassment, frustration	3
2.07	Requires me to take action and fix	2
2.08	I lose confidence in the information	1
2.09	My workload will increase	1
	Sub-total	**21**
3	**RISK PERCEPTIONS RELATING TO OTHERS**	
3.01	Their trust/respect/confidence in us is diminished	3
3.02	Customer service drops	5
3.03	Customer costs increase	0
	Sub-total	**8**
4	**WHY I THINK IT'S A RISK**	
4.01	Existing controls and safeguards are inadequate	13
4.02	Happens a lot	4
4.03	Malicious/sinister/intentional	2
4.04	Internal/External perpetrator	2
4.05	Significant wide ranging impact/lots of people affected	5
4.06	Damage unknown	4
	Sub-total	**30**
5	**MISCELLANEOUS**	
5.01	Irrelevant	1
	Sub-total	**1**
	Total	**98**

Content Analysis

This study used the Honey (1979a) content analysis method as described in Jankowicz (2004). This method makes use of the IS risk perception categories shown in Table 1 above and claims to be superior to most other methods in that it does not lose any of the constructs or the ratings across the threat elements by the process of averaging. Another advantage of this method is that it makes use of the supplied overall bipolar construct that is common to every grid, "*Overall, less risky ----- Overall, more risky"*.

This method involved the development of a spread sheet table for the combined group of 12 interviewees. This table was then converted into a bar chart to highlight the most important, that is, the most significant risk perception categories for the group (Refer Figure 2 in the Results section).

Principal Component Analysis (PCA)

Each of the 12 interviewee repertory grids was subjected to a PCA using the GRIDSTAT version 5 software (Bell 2009). For each PCA, the number of components to extract was determined by the researcher at the time of generation using the "Eigenvalues-greater-than-one" rule (Velicer 1976). The researcher also chose to use the Varimax Orthogonal Rotation method to identify two or three principal components from each grid. In total, 31 components were generated by the 12 PCAs.

The next step was to develop an a priori set of labels that could be assigned to non-ambiguous components. After scouring the literature (Fischhoff, Slovic, Lichtenstein, Read and Combs 1978 ; Jenkin 2006 ; Slovic, Fischhoff and Lichtenstein 1980) for factors that influence people's perceptions of IS risks it was decided to use properties or characteristics of IS risks since this study focussed on perceptions of IS risk. Jenkin (2006) refers to such factors as situational factors and the following were chosen as the most suitable for this study:

- Type of Loss;
- Personal Impact;
- Severity/Scope;
- Cause/Intention;
- Controllability/Preventability and
- Resolvability.

The 31 components that were generated from the 12 PCAs were allocated one of these labels provided the constructs that comprised the component were consistent with the meaning of the label; otherwise the component was labelled as "Ambiguous" (Refer Table 2 in the Results section).

RESULTS

Identification of IS Risk Perceptions

The results of the content analysis (Honey 1979b) of the 12 RGT interviews are represented by the bar chart shown in Figure 2 below. Constructs were weighted according to how well they correlated with the overall riskiness construct, "*Overall, less risky ----- Overall, more risky"*. Highly correlated constructs were given a weight of three, medium correlated constructs were given a weight of two and low correlated constructs were given a weight of one.

As can be seen from the bar chart below, the interviewees considered the following IS risk perceptions to be the most important and significant:

- 4.01 Existing controls and safeguards are inadequate
- 1.06 Systems down/unable to access information/reduced productivity
- 1.03 Increases costs/requires additional resources
- 2.03 I can't do my job properly

Interestingly, the risk perception category, 4.01 (shown shaded in the bullet list above) is not a perception of risk but is a perception of why interviewees thought particular threats were a risk. In other words, theme number four "Why I think it is a risk" contains categories that do not represent what the organisation (or computer user or other stakeholder) stands to lose. Instead, these categories represent the reason that certain threats pose a risk to

organisations. These perceptions were included in this study because they were genuine perceptions of the local government participants. Consequently, this study revealed, albeit serendipitously, that the most significant perception of the local Government participants was that their organisation's existing IS controls and safeguards were inadequate to ensure an acceptable level of InfoSec. If this typical misinterpretation and confusion between risks and threats is ignored for the moment, the research indicates that interviewees considered that the most serious risk to their organisation's IS is that systems will become unusable or unavailable such that large costs would be incurred to restore services and maintain productivity. Interviewees were also concerned that they would not be able to do their job properly if they could not get access to information.

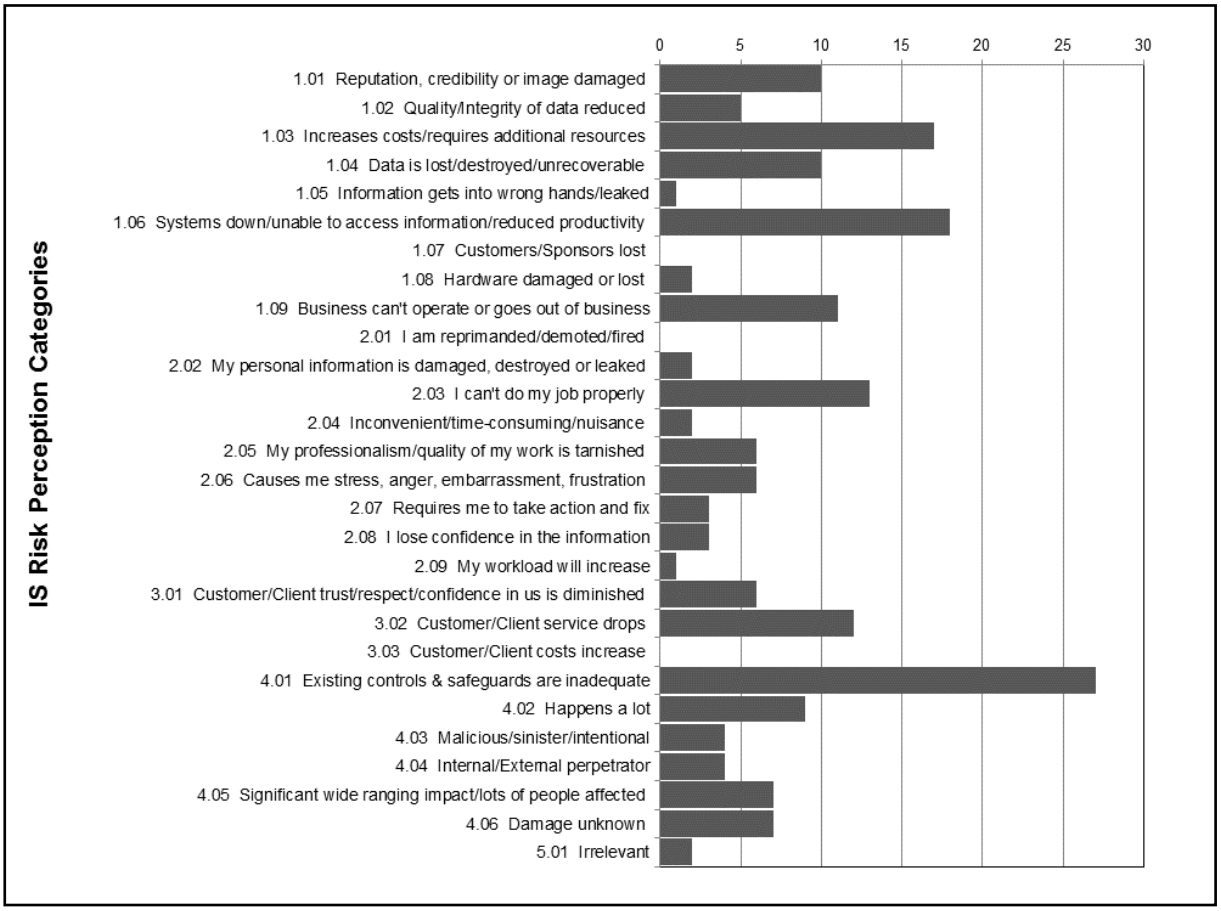

Figure 2: Weighted IS Risk Perceptions

The bar chart in Figure 2 above also highlights the risk perceptions that do not concern local government employees and the major ones were:

- 1.05 Information gets into wrong hands/leaked
- 1.07 Customers/sponsors lost
- 2.01 I am reprimanded/demoted/fired
- 2.09 My workload will increase
- 3.03 Customer/client costs increase.

As with the list of 'the most significant IS risk perceptions of computer users', the list of 'the least significant IS risk perceptions' needs to be considered within the context of the research participants being employees of a local government organisation. It is not necessary for local government organisations to maintain a level of security comparable to that of Defence organisations or financial institutions that demand the highest levels of InfoSec. This is because the data stored and processed by a bank, for example, is far more attractive to hackers and criminals than the data held by a local government organisation. As a consequence, local government employees can be excused for thinking that their organisation's information is not particularly valuable or sensitive. This could explain why participants did not perceive any risk that their customers' or client's costs would increase; or

any risk of losing customers/sponsors; or any risk that they might be reprimanded, demoted or fired for causing such breaches of InfoSec.

Identification of Situational Factors

An analysis of the components that were shown to have the principal influence on interviewee IS risk perceptions is shown in Table 2 below. For example, the IS risk perceptions of interviewee number one appear to be influenced by the severity and/or scope of the impact of potential threats. Interviewee number eight, on the other hand, was influenced most by the type of loss that would be incurred by the impact of threats, and to a lesser extent influenced by the severity and/or scope and also by the controllability and/or preventability of potential threats.

Table 2: Principal Component Analysis and Situational factors

Grid No.	No. of Constructs	Overall IFS	Component 1	%age variance	Component 2	%age variance	Component 3	%age variance
1	9	0.88	Ambiguous	41.45	Severity/Scope	39.74	X	
2	8	0.66	Ambiguous	47.28	Ambiguous	44.47	X	
3	9	0.72	Ambiguous	44.25	Personal impact	36.18	X	
4	9	0.78	Ambiguous	28.98	Ambiguous	32.48	Type of loss	24.29
5	8	0.90	Ambiguous	34.81	Type of loss	21.45	Ambiguous	21.90
6	9	0.84	Ambiguous	35.47	Ambiguous	26.49	Type of loss	20.18
7	4	1.00	Ambiguous	70.95	Personal impact	25.14	X	
8	11	0.78	Type of loss	40.28	Severity/Scope	28.26	Controllability/ Preventability	15.97
9	9	0.78	Ambiguous	29.53	Type of loss	27.57	Type of loss	24.23
10	9	0.75	Ambiguous	27.75	Type of loss	27.15	Type of loss	30.42
11	9	0.75	Ambiguous	31.94	Ambiguous	33.12	Ambiguous	21.57
12	4	0.81	Type of loss	41.73	Type of loss	35.80	X	

Examination of the data in Table 2 above suggests that for the overall group of local government employees, the component that has the most impact on individual IS risk perceptions is the situational factor "Type of loss". This situational factor refers to the "type" of impact (not severity of impact or extent of loss!) that could be caused by a security threat. For example, this could be loss of data or corruption of data; reputation or image damage; loss of clients or customers; increased costs; reduced productivity; business can't operate or reduction of services. In this study the most significant type of loss was perceived to be "reduced productivity that caused an increase in costs".

This finding is confirmed by the Kaiser (1974) Index of Factorial Simplicity (IFS) for each grid, which indicates that the quality of the components is relatively high (refer 2nd column of Table 2 headed "Overall IFS"), and also by the aggregation of the percentages of variance attributed by the "type of loss" component compared to the other components.

The results outlined above relate to the interviews of 12 employees of a single local government organisation, and as such, cannot be generalised to employees in non-local government organisations. Consequently, similar interviews were conducted with computer users employed at organisations that included a university department, a state government agency, a federal government department, a publishing company and a large accounting firm. Interestingly, the results for local government employees were generally a reflection of the overall results for all participant organisations, with one exception. Even though the local government employees acknowledged that

their organisation was at risk of damage to their reputation, credibility or image, they did not place as much significance on this risk compared to employees from other types of organisation. This was a concern for local government management.

CONCLUSIONS

This paper reports on a study that addresses a particular human aspect of InfoSec that has been and continues to be a major concern of senior management, namely, the behaviour of employees whilst they are using a computer. Although this research did not examine computer-user behaviour per se, it focussed on individual IS risk perceptions of employees on the understanding that better perceptions of the risks to organisational computer systems will help to make computer-user behaviour more risk-averse (and therefore less risky).

The aim of this research was to examine how computer users perceive the risks to their organisation's IS. More specifically, the aim of this paper is to report on the IS risk perceptions of computer users within a local government organisation and to indicate how these perceptions were influenced by situational factors such as severity of impact of a security breach, beliefs about the cause of the risk and the nature of the perpetrators.

In summary, the research methods of categorising perceived IS risks and conducting a content analysis of the RGT interview data revealed that the major IS risk perception of local government computer users was that the existing IS controls and safeguards were inadequate in providing an appropriate level of InfoSec. Notwithstanding the fact that "inadequate controls" is not a risk but a threat, this research showed that local government employees perceived the risk of their organisation's IS becoming unusable or unavailable (such that large costs would be incurred to restore services and maintain productivity) to be the most significant. They also perceived that their inability to do their job properly due to information being inaccessible was a substantial IS risk. The research results also highlighted IS risk perceptions that were not rated very highly by the participants. These results were potentially interesting to senior management, however, most of these were considered to be a product of the local government environment except for the perceived risk of damage to the organisation's reputation, credibility or image, which was rated quite low. A principal component analysis of the RGT data confirmed that the component that has the most impact on local government employee IS risk perceptions is the situational factor "Type of loss".

Armed with this information, senior management is better placed to manage their InfoSec more effectively by designing and implementing intervention activities such as training sessions, risk communication seminars and InfoSec policy compliance audits that emphasise the various types of loss that their organisation can suffer. For example, an InfoSec awareness session that focusses on the importance of maintaining a local government's reputation and trust may be more effective than communicating the potential impact of a myriad of InfoSec threats.

REFERENCES

Bell, R. 2009. "Gridstat: A Program for Analyzing the Data of a Repertory Grid", Department of Psychology, University of Melbourne, Victoria, Australia.

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

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*, (2008:23), pp. 37-62.

Essau, C. 2004. "Risk-taking Behaviour among German Adolescents", *Journal of Youth Studies*, (7:4), pp. 499-512.

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*, (9:2), pp. 127-152.

Gill, M. 1994. *Psychoanalysis in Transition: A personal view*, Analytic Press, Inc.

Honey, P. 1979a. "The Repertory Grid in Action", *Industrial and Commercial Training*, (11), pp. 452-459.

Honey, P. 1979b. "The repertory grid in action: How to use it to conduct an attitude survey", *Industrial and Commercial Training*, (11:11), pp. 452-459.

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

Jenkin, C. 2006. "Risk perception and terrorism: Applying the Psychometric Paradigm", *Homeland Security Affairs*, (2:2), pp. 1-14.

Johnston, A. and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study", *MIS Quarterly*, (34:3), pp. 549-566.

Kaiser, H. 1974. "An Index of Factorial Simplicity", *Psychometrika*, (39:1), pp. 31-36.

Katapodi, M., Lee, K., Facione, N. and Dodd, M. 2004. "Predictors of perceived breast cancer risk and the relation between perceived risk and breast cancer screening: a meta-analytic review", *Preventive medicine*, (38:4), pp. 388-402.

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

Lapidus, J., 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 & Prevention*, (18:6), pp. 546-559.

Lee, Y. and Larsen, K. 2009. "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-malware Software", *European Journal of Information Systems*, (18:2), pp. 177-187.

Machin, M. and Sankey, K. 2008. "Relationships between young drivers' personality characteristics, risk perceptions, and driving behaviour", *Accident Analysis & Prevention*, (40:2), pp. 541-547.

Magklaras, G. and Furnell, S. 2005. "A preliminary model of end user sophistication for insider threat prediction in IT systems", *Computers & Security*, (24:5), pp. 371-380.

Moynihan, T. 1996. "An inventory of personal constructs for information systems project risk researchers", *Journal of Information Technology*, (11:4), pp. 359-372.

Napier, N., Keil, M. and Tan, F. 2009. "IT project managers' construction of successful project management practice: a repertory grid investigation", *Information Systems Journal*, (19:3), pp. 255-282.

Pahnila, S., Siponen, M. and Mahmood, A. 2007. "Employees' Behavior Towards IS Security Policy Compliance," 40th Hawaii International Conference on System Sciences (HICSS'07), IEEE Computer Society Press, Los Alamitos, California.

Reger, R. 1990. "The repertory grid technique for eliciting the content and structure of cognitive constructive systems" in: *Mapping Strategic Thought,* A. Huff (ed.), John Wiley & Sons Chichester, NY, USA, pp. 301-309.

Siau, K., Tan, X. and Sheng, H. 2010. "Important characteristics of software development team members: An empirical investigation using Repertory Grid", *Information Systems Journal*, (20:6), November 2010, pp. 563-580.

Slovic, P., Fischhoff, B. and Lichtenstein, S. 1980. "Facts and fears: Understanding perceived risk", *Societal risk assessment: How safe is safe enough*), pp. 181-216.

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

Tan, F. and Gallupe, R. 2006. "Aligning business and information systems thinking: a cognitive approach", *IEEE Transactions on Engineering Management*, (53:2), pp. 223-237.

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

Tan, F. and Tung, L. 2003. "Exploring website evaluation criteria using the repertory grid technique: A web designers' perspective," Proceedings of the Second Annual Workshop on HCI Research in MIS, AIS, Seattle, WA, USA.

Tomico, O., Karapanos, E., Lévy, P., Mizutani, N. and Yamanaka, T. 2009. "The Repertory Grid Technique as a Method for the Study of Cultural Differences", *International Journal of Design*, (3:3), pp. 55-63.

Velicer, W. F. 1976. "Determining the number of components from the matrix of partial correlations", *Psychometrika*, (41:3), pp. 321-327.

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

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

Williams, D. and Noyes, J. 2007. "How does our perception of risk influence decision-making? Implications for the design of risk information", *Theoretical Issues in Ergonomics Science*, (8:1), pp. 1-35.

COPYRIGHT