RISK COMMUNICATION, RISK PERCEPTION AND INFORMATION SECURITY

Malcolm Pattinson[1] and Grantley Anderson[2]
[1]*University of South Australia, malcolm.pattinson@unisa.edu.au;* [2]*Anderson Analyses, grantley.anderson@bigpond.com.au*

Abstract: This paper puts forward the view that an individual's perception of the risks associated with information systems determines the likelihood and extent to which she or he will engage in risk taking behaviour when using a computer. It is suggested that this behavior can be manipulated by 'framing' a communication concerning information system risk in a particular manner. In order to achieve major effectiveness in getting an information security message across to a computer user, this paper discusses and demonstrates how his or her individual cognitive style should be considered when framing the risk message. It then follows that if the risk taking behaviour of computer users becomes less risky due to an increase in the level of perceived risk, then the level of information security increases.

Keywords: Information Security, Risk Perception, Risk Communication, Field-Dependent (FD), Field-Independent (FI), Framing.

1. INTRODUCTION

For too long now, the information security fraternity, and indeed management, have focused their attention on hardware and software solutions in their attempt to mitigate against risks to their information systems. We are now starting to see this focus change slightly with the realisation that people issues are equally important. Backhouse et al, (2004) and Jackson, et al, (2004) are two such papers that draw attention to the social aspects of information systems and the security surrounding them. It is a universally accepted fact that IT/IS people are an important component of any information system. One only has to look at the relevant textbooks for a definition of 'information system' to realise that people are one of the five components that comprise an information system. The other components are hardware, software, data and procedures.

This paper is concerned with the perception that computer users have of the risks to the information systems. For example, when someone asks "What is the risk of your computer getting a virus - is it high, medium or low?" What do you say? What they are really asking you is "What is your individual perception of the risk?" (Note that 'actual' information systems

risks can never be measured - risks are intangible and subjective and can only be estimated). What influences your answer - past experience, knowledge about viruses, recent media reports or your mood on that day?

It is suggested that, although these factors and others have a bearing on your response (that is, your perception), so does the way that the question is phrased. If the question was rephrased as "What is the risk of your computer getting a virus and causing havoc for many colleagues - is it high, medium or low?". Does this 'reframing' and provision of additional information influence your answer and therefore your perception of the risk? The answer to this question is the crux of this paper.

2. RISK PERCEPTION

The manner in which people see the risks associated with information security determines what decisions they will make regarding the actions they will take (or not take) in conjunction with whatever risk security measures their particular organisation has put in place. Unfortunately, to date, not much is known about the perceptions that computer users hold concerning information systems risk.

However, research into risk perception in general has identified some important factors. The influence these factors have on risk perception is considered to be a function of the extent to which the risk is viewed as (a) voluntary, (b) under control, (c) representing a threat or catastrophe, or (d) having potential for a reduction in gains, or an increase in losses (Heimer, 1988).

The literature on risk perception seems to be devoid of research into its prevalence in the information security domain. However, in terms of general risk perception research, there is an abundance of articles and studies that look at factors that influence risk perception. For example, Bener (2000) claims that there is a range of social, cultural and psychological factors that contribute to risk perception. Furthermore, Otway (1980) lists other factors that shape risk perception such as the information people have been exposed to, the information they have chosen to believe and the social experiences they have had, to name a few.

One of the factors that is purported to have an influence on risk perception is the way in which the risk message is communicated to computer users and IT management. Bener, (2000) is one such author that supports this view, and he claims that risk is communicated within an organisation that contributes to the risk perception of the different individuals within that organisation. It then follows that if people's perception of risk is changed, there is the likelihood that their risk-taking

behaviour will change. If this behaviour changes for the better, then it can be argued that the actual risk is lessened.

3. RISK COMMUNICATION

Risk communication has been defined by numerous authors. For example, (O'Neill, 2004) defines it as"...an interactive process of exchanging information and opinions between stakeholders regarding the nature and associated risks of a hazard on the individual or community and the appropriate responses to minimise the risks. The key behavioural change lies in risk communication designed to change people's perception of the risk and to increase their willingness to manage the risk." (p. 14).

Similarly, the US National Research Council, (1989) defines it as "an interactive process of exchange of information and opinion among individuals, groups and institutions. It involves multiple messages about the nature of risk and other messages, not strictly about risk, that express concerns, opinions and reactions to risk messages or to legal and institutional arrangements for risk management" (p. 21 as cited in Bener, 2000 & Backhouse et al, 2004).

The media plays a significant role in influencing people's perception of information system risk. One only has to look at the impact of the terrorist attack on the world trade centre twin towers on September 11, 2001. Another example is the reporting of the phishing software that logs keystrokes and subsequently gains banking information including user name and password.

The challenge with any form of risk communication is how to target a specific audience. For example, computer users, the subjects of this proposed research, range from executives through to general users through to IT experts, all of which have a different understanding and appreciation of information system risks. One approach, as described by O'Neill, (2004), is to divide the world's population into four types, namely, those who are risk averse, those who are risk tolerant, people who deny risk and people who seek out risk and then target each of these groups with different messages.

Alternatively, one could target individuals rather than groups, as put forward in this paper, by phrasing information security 'messages' to suit the individual. This internationally accepted approach is called 'message framing' or just 'framing'.

4. FRAMING

Framing is a concept that relates to the way a set of facts or a situation is described by a communicator. It also relates to a type of cognitive set that the receiver of a communication may use in order to interpret and make sense of any communication that he or she receives. From the point of view of the receiver, the way in which a message is framed as it is received will have an impact upon the course of action that he or she will choose to undertake.

In terms of risk communication effectiveness, the way a message is framed by a sender has significant potential to set decision boundaries in that it may determine what is included and what is left out of consideration by the receiver. Of even greater significance is the fact that not all the "in" elements will receive the same attention. A receiver's framed message tends to focus the individual on certain elements in a situation, while leaving other elements either unexamined, or at best, relatively obscured (Russo & Schoemaker, 1989).

Consider a risk communication written (or framed) in two different ways in two different messages. In the first message the aim is to provide an explanation of a potential event that threatens the security of an organisation's computer systems, such as a computer virus that has the potential to wipe out critical data files stored on hard disk. For example, one approach might be to phrase the message such that the emphasis is on how such an event will cause the organisation's technical competence to come into question as well as causing substantial costs to be incurred.

In the second message of the communication, information is provided as to what each individual computer user must do in order to ensure that the organisation's information security protocols have been properly implemented and observed. For example, the communication would be phrased in such a way that the emphasis is on how the prevention of such a security breach can be achieved by individual computer users exerting some effort in following a set of laid down procedures designed for that purpose.

Numerous studies (Tversky & Kahneman (1981), McNeill et al (1982), Meyerowitz & Chaiken (1987) on framing support the view that the way a situation is framed can have a substantial impact on people's risk taking behaviour. However, it is our belief that what should be of particular interest to information security managers and supervisors relates to more than just the general finding that people are more inclined to take risks in order to avoid losses than they are to take risks in order to make gains. Rather, it is the finding, derived mainly from the educational literature, that the importance placed on a particular message by an individual may be as much

influenced by that person's cognitive style, as it is influenced by the core content of the message (Chinien, 1990).

We believe this distinction to be an important one. Principally because one of the surprising findings of this proposed research into human factor problems associated with information security procedures, is that very little has been written about individual differences in the way that individual computer users process information that has been presented to them, be that by hard copy written communications or by computer interface methods. Consequently, it would not be surprising to find that few information security managers and supervisors are aware that human information processing factors are predominately a consequence of an individual computer user's personal cognitive style.

5. COGNITIVE STYLE

As a personality dimension, an individual's cognitive style has a significant impact on the way that she or he collects and interprets information that is presented to her or him. Cognitive style is not considered to be a fixed personality trait, rather it is viewed as the preferred and habitual approach that an individual adopts when organising and presenting information. A number of such styles are described in the literature. However, since it describes how effectively an individual is able to restructure information using salient cues and field arrangements, for our purposes the dimension of Field Dependence versus Field Independence seems the most appropriate one to discuss and examine.

FD/FI has been researched extensively (Witkin et al, 1997; Ausburn & Ausburn, 1978) and is an established construct in the domain of psychology.

Why is this personal characteristic important? The focus of this paper is on the perception of risk and although the way that people perceive risks is a complex sociological and psychological phenomenon, the authors of this paper are suggesting that one way of changing individual risk perceptions is to communicate in a way that is aligned to each individual's FD/FI cognitive style. The aim of this proposed research is to determine whether the framing of potential threat scenarios has an effect on computer user risk perception, particularly if the threat scenarios are framed in an FD sense for FD people and an FI sense for FI people.

Much of the literature on framing refers to wording a situation in terms of potential gains and potential losses. In particular, a substantial amount of this literature relates to the medical profession, such as the Meyerowitz & Chaiken (1987) research into the effect of a negatively worded (or gain-

frame) pamphlet versus a positively worded (loss-frame) pamphlet about breast self-examination.

But framing doesn't only relate to wording a situation in terms of potential gains and losses. It can also refer to elements such as:

- how it affects the subject
- self justification or previous action
- support investment already made
- social benefits and costs
- self image
- organisational image
- reputation
- face saving

Table 1. Summary of the FD/FI cognitive style construct

Individuals classified as FD	Individuals classified as FI
Drawn to people	Enjoys own company
Like to have people around them	Not sensitive to others around them
More non-verbal behaviours	Less non-verbal behaviour
Prefer occupations which require involvement with others	Prefer occupations with less interaction
Take a longer time to solve problems	Solve problems rapidly
Alert to social cues	More aloof, theoretical
Highly developed social skills	More abstract & analytical
Sensitive to social criticism	Initially thought to be males but inconclusive
Extremely influenced by others	Less inclined to be influenced
Teachers	Prefer maths & physical sciences
Global way of perceiving	Analytic way of perceiving

So, how might we frame the explanation of a potential threat and its impact to the two different types of cognitive styles, field-independent and field-dependent so that their level of perceived risk is raised?

6. FRAMING MESSAGES IN TERMS OF FD/FI

The aim of this research is to show that when the explanation of a potential threat scenario is couched in a way that is in line with an

individual's cognitive style, then that individual is likely to perceive the risk to be higher than if the explanation was framed differently.

Therefore, for FD types, the potential threat scenario should be framed in a way that highlights:

- the global impact,
- the social implications,
- the impact it would have on people/individuals,
- what individuals can do to mitigate against the risk,
- the benefits to individuals
- how we might be viewed by others or
- how our image might suffer.

Conversely, for FI types, the potential threat scenario should be framed to emphasise:

- physical effects
- a practical/pragmatic solution to the problem with little regard to the impact on people
- a quick fix solution
- hardware and/or software solutions

The following three threat scenarios have been framed according to the FD/FI cognitive style.

Table 2. Threat Scenario No. 1 - Theft of desktop computer

Written for FD's	**Written for FI's**
Your office was broken into and a desktop computer was stolen by an unknown external person. Sensitive information could be leaked to unauthorised people that could be embarrassing for the organisation. Depending on your backup procedures, this could be costly for the IT department to recover.	Your office was broken into and a desktop computer was stolen by an unknown external person. You will be without a computer until a replacement can be purchased. You may have to use one of the office laptops in the meantime. Recovery of all data could be difficult if you did not backup everything.

Table 3. Threat Scenario No. 2 - A virus infection

Written for FD's	Written for FI's
Your office desktop computer has been infected with a virus. If not addressed immediately, it might spread through the whole organisation, causing inconvenience and loss of productivity. It may damage people's hard drives, causing valuable & sensitive information to be lost. This would be embarrassing for the organisation.	Your office desktop computer has been infected with a virus. If not addressed immediately, it could damage your computer files preventing you from doing your work. This could be embarrassing for you because you obviously did not run anti-virus software properly.

Table 4. Threat Scenario No. 3 – A software bug

Written for FD's	Written for FI's
An accidental software bug in one of our application programs could cause our computer system to crash. This, in turn, could cause a delay in processing the fortnightly pays, or prevent invoices from being processed on time. Futhermore, employee confidence in the computer system could be impacted.	An accidental software bug in one of our application programs could cause our computer system to crash. To prevent this breach from occurring in the future, we have to tighten up our testing procedures to ensure that all programs are thoroughly tested before they are put into production.

7. CONCLUSION

The primary aims of this paper were, firstly, to emphasise the importance of human factors/behaviour as management strive for an acceptable level of information security within their organisations. The second aim was to present a risk communication approach, namely cognitive style framing, that management might consider in an attempt to change user risk-taking behaviour of computer users at all levels. It is suggested that a positive change of this nature can reduce the level of risk.

This paper supports the view that an acceptable level of information security is best achieved by addressing all components of an information system, particularly issues relating to the people component. It also attempts to contribute to an ever-increasing amount of research into the sociological aspects of risk as it relates to the domain of information security. Also examined is the concept that better risk communication, by deploying the concept of framing, will mitigate against the actual information risks as depicted in Figure 1 below.

This is essentially a theory paper. However, the authors expect to present some preliminary findings of a pilot study to sample test a range of threat scenarios at the IFIP WG11.1 conference in December 2005.

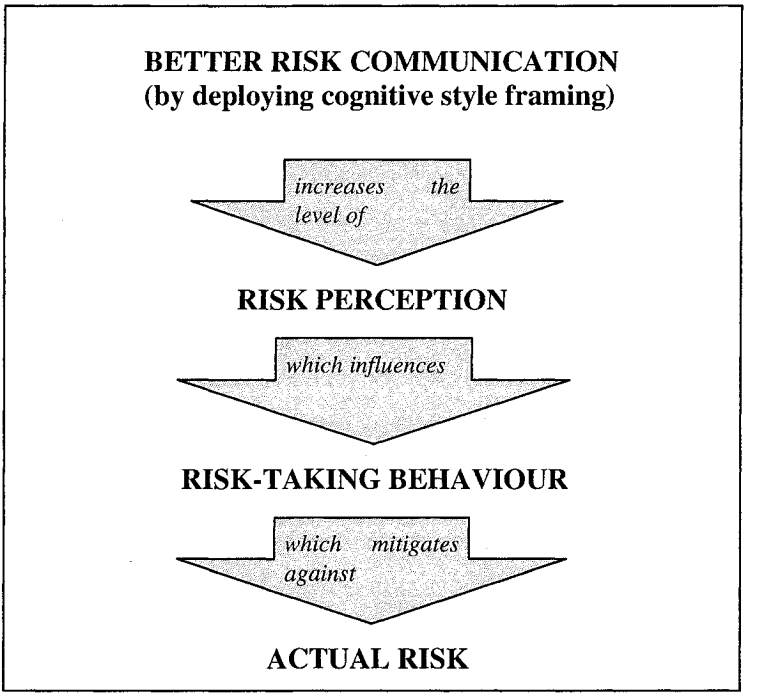

Figure 1.

8. REFERENCES:

Backhouse J., Bener A., Chauvidul N., Wamala F. & Willison R., 2004, "Risk Management in Cyberspace", Available at http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/, viewed 27 April 2005.

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.

Chinien, C. A., 1990, "Examination of Cognitive Style FD/FI as a Learner Selection Criterion in Formative Evaluation", *Canadian Journal of Educational Communication*, Vol 19, pp. 19-39.

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

Heimer, C. A., 1988, "Social Structure, Psychology, and the Estimation of Risk", *Annual Review of Sociology*, Vol 14, pp. 491-519.

Jackson J., Allum, N. & Gaskell, G., 2004, "Perceptions of Risk in Cyberspace", Available at http://www.foresight.gov.uk/Previous_Projects/Cyber_Trust_and_Crime_Prevention/Reports_and_Publications/, viewed 27 April 2005.

Johnson C., 2002, Available at http://www.dcs.gla.ac.uk/~johnson/teaching/safety/open_assessments/assess2002.html, viewed 28 July 2004.

McNeil B. J., Pauker S. G., Sox H. C. & Tversky A., 1982, "On the Elicitation of Preferences for Alternative Therapies", *New England Journal of Medicine*, Vol 306, pp 1259-1262.

Meyerowitz B. E. & Chaiken S., 1987, "The Effect of Message Framing on Breast Self-examination Attitudes, Intentions and Behaviour", *Journal of Personality and Social Psychology*, Vol. 52, No. 3, pp 500-510.

O'Neill P., 2004, "Developing A Risk Communication Model to Encourage Community Safety from Natural Hazards", paper presented at the Fourth NSW Safe Communities Symposium, Sydney, NSW.

Otway H. J., 1980, "Risk Perception: A Psychological Perspective", *Technological Risk: Its Perspective and Handling in Europe*, M. Dierkes, S. Edwards & R. Coppock.

Russo J. & Schoemaker, P. J. H., 1989, *Confident Decision Making*, London, Piaktus Press.

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

Tversky A. & Kahneman D., 1981, "The Framing of Decisions and the Psychology of Choice", *Science*, Vol. 211, pp 243-248.

Wilson R. M. S., 2001, "The Framing of Financial Decisions: A pilot study", *Research Series Paper 2001:3*, ISBN 1859011713, Loughborough University.