How Well Are Information Risks Being Communicated To Your Computer End-Users?

M. Pattinson[1] and G. Anderson[2]

[1] University of South Australia, Australia
[2] Anderson Analyses, Australia

Abstract

The authors of this paper adopt the premise that an individual's perception of the risks associated with information systems significantly influences the likelihood and extent to which she or he will engage in risk-taking behaviour when using a computer. Furthermore, they believe that the manner in which information system risks are communicated to the computer end-user can affect a change to his or her perception of the risks. Although there are numerous ways in which the communication of risk can be manipulated, this paper focuses on the use of graphics and symbols embedded within information security risk messages. Also outlined is some preliminary research conducted by the authors in an attempt to provide some much-needed evidence-based research relating to human aspects of information security and assurance.

Keywords

Information Security (InfoSec), Risk Perception, Risk Communication, Semantic Differential (SD).

1. Introduction

The "Conference Concept" for the inaugural international conference on Human Aspects of Information Security and Assurance, July 2007 states:

"It is commonly acknowledged that security requirements cannot be addressed by technical means alone, and that a significant aspect of protection comes down to the attitudes, awareness, behaviour and capabilities of the people involved……Ensuring appropriate attention and support for the needs of users should therefore be seen as a vital element of a successful security strategy." (HAISA, 2007).

We seem to have reached a point in the information security (InfoSec) lifecycle where considerable literature exists that asserts that there is more to managing information security than simply focusing on hardware and software vulnerabilities.

Authors such as Schneier (2000 & 2004), Pincus (2005), Heiser (2005) and numerous others have been saying for a number of years that human factor aspects are equally important, if not more important, in terms of achieving an acceptable level of information security within an organisation.

To the present authors it appears that the above assertion is more often proclaimed a fact than is actually shown to be the case with the support of empirical evidence. For many researchers it is as though it were sufficient to nod in the general direction of human factors as a casual explanation, without necessarily delineating precisely what type of human factors under exactly what type of circumstances are likely to have a significant impact.

Some human factors that have the potential to impact upon the security of an organisation's information systems are:

- ∉ Organisational policy & risk culture
- ∉ Individual propensity to take risks
- ∉ The theory of risk homeostasis
- ∉ The bystander affect
- ∉ Familiarity with the communication
- ∉ Individual perception of the risks
- ∉ Age, gender, position in the organisation
- ∉ Cost of compliance
- ∉ Amount of education & training
- ∉ Individual cognitive style
- ∉ Experience
- ∉ How well the risks are communicated

Some of these factors relate to surroundings and conditions, some are considered sociological and others are related to the person's upbringing, culture or experience. This list is by no means exhaustive, and furthermore, this paper does not attempt to address all of these factors, but focuses on only two, namely, individual perception of the risks and how well these risks are communicated.

More specifically, the focus of this paper is more on the risk perceptions of computer end-users than it is on their risk-taking behaviour. The principle premise being that if computer end-user perceptions of the risks associated with information security threats are heightened, then it is likely they will exhibit more desirable behaviour.

Consequently, the aim of this paper is twofold. The first aim is to present the argument that the manipulation of risk communications by incorporating human factor variables can influence the information risk perceptions of computer end-users. In turn, this has the potential to improve end-user risk-taking behaviour. The second aim of this paper is to describe and discuss some pilot study research that attempts to ascertain whether the embedding of symbols or graphics within information security messages achieves a positive shift in the risk perceptions of computer end-users.

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 security measures their particular organisation has put in place. Unfortunately, to date, not much is known about the perceptions that computer end-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 are a number 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. Additionally, 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 but a few.

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 acquires IDs and passwords to enable access to banking information.

A good practical example of risk perception relates to the process of backing up our personal data. Assume that you are writing a large, but very important business report for your senior management and it is taking many days and much research effort. How often do you backup your work? What is your perception of the risk that you could lose all the good work you have done because of some computer problem or whatever? Some people have no appreciation of the intricacies of a computer and what can go wrong - these people are blithely unaware of the risks of losing everything. Yet it has probably happened to all of us at least once!

On the other hand, there are also informed people who are aware of the unpredictability of computers and that they sometimes crash for no apparent reason. Such people will back up regularly and to various mediums. In the end, we do personal backups to the extent that we are confident that we won't lose anything or any time. This is where we differ as individuals. Some people are risk-takers by nature and feel that they can rely on the automatic server backup that occurs every hour. On the other hand, some of us are more conservative and backup almost too often, just to be sure.

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 end-users and IT management. Bener, (2000) claims the manner in which risk is communicated within an organisation substantially influences the risk perception of the different individuals within that organisation. Lippa (1994) put forward a similar view, claiming 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.

3. End-user Risk-taking Behaviour

For the purposes of this paper, the term 'end-user risk-taking behaviour' refers to behaviour that ranges from the very risk averse (or very good) behaviour through to the very risk-inclined (or very bad) behaviour and can be either deliberate or accidental. A selection of such behaviours is shown below:

Risk-averse behaviour (deliberate)	**Neutral 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

Recent research by Stanton, Stam, Mastrangelo & Jolton, (2005) analysed the various types of computer end-user behaviour and developed a taxonomy of six behaviour categories which can be aligned to the columns above as:

Aware Assurance Basic Hygiene	Dangerous Tinkering Naïve Mistakes	Intentional Destruction Detrimental Misuse

4. Risk Communication

As with other aspects of risk in general, risk communication has been variously 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 USNRC, (1989) defines risk communication 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).

For some time, the importance of communicating risk effectively has been of concern to those in the health industry, particularly in relation to risks in pharmacotherapy. Coleman (2005), in a paper on presenting information on risks associated with prescribing medicines and drugs, sees appropriate risk communication "as one of the most important approaches used today to minimise risk" (p. 513). He strongly advocates that the presentation of information on risks should be as simple and as user-friendly as possible. Although Coleman is referring to risk information relating to medication and drug therapy, the present authors believe that these principles are also applicable to risks relating to information security.

Potential threats and their subsequent risk to an organisation's information systems need to be communicated to all levels of computer end-users, from the order clerk to the application developer to the IT support person to senior management and the C-suite executives. Some common forms of risk communication include, for example:

Security awareness seminars
Standard email memos
Notice board memos
Phone calls
Web pages
One-on one discussions
Group meetings
Flyers

There is a constant problem for anyone designated with the task of organising such activities. Namely, what might have proven to be an appropriate technique in a one-on-one discussion may not necessarily prove to be as useful in an email message or a seminar presentation. In other words, different forms of risk communication require a considerable amount of thought by the sender in terms of how to achieve maximum effectiveness when he or she uses a particular communication medium.

Furthermore, it should be noted that the impact of a communication pertaining to a risk or a hazard is not always a direct result of the design of that communication. There are a number of additional factors that can render a message to be ineffectual. For example, familiarity with the message, that is, repeated exposure to the message, has been shown to create automatic behaviour and a total disregard for the message. This phenomenon is sometimes referred to as 'experience with the message' and gives the impression of apathy. Similarly, the issue known as 'cost of compliance' can also appear to be end-user apathy when in fact the person may have made a conscious decision not to take heed of the message regarding a risky situation (OSHA, 1997; Visual Expert, 2003). These two issues are appreciated by the authors but are beyond the scope of this paper, which is predominantly concerned with how we might communicate risk better.

5. Communicating Risk with Graphics & Symbols

The topic of 'effective presentation of information' has been extensively studied and researched for many years in many diverse environments. In particular, marketing professionals are well versed in the styles and methods that can be used to 'get the message across' to consumers, customers, boards of management, etc. Also, educationalists have conducted a plethora of research relating to the presentation of information in an attempt to improve learning outcomes. One of these techniques is to use appropriate symbols, pictures, graphics, colours etc embedded within advertisements, reports, memos, emails and presentation slides. The design of children's books is another example of how symbols and pictures can be used to maximise the understanding by the reader (Bang, 1991).

There is no apparent evidence of literature relating to the presentation of information concerned with the topic of information security risk. If risk communication is such an important tool in mitigating information risks, then it seems that there is a current hiatus in this research area. What is the most effective means of sending a broadcast email to all staff? How should it be worded?, how often should it be sent?, when should it be sent?, what colour should the font & background be? These questions and many more need answers based on sound theory supported by relevant empirical evidence in a typical evidence-based research approach that is most predominant in the field of health care.

The following sections detail some of the more recent field work the present authors have conducted, focusing almost entirely on the presentation of email messages that incorporate a graphic or symbol within the main body of the message. The impetus for this work was the observation that email communications being sent to computer end-users about information security issues and warnings tended to be almost exclusively concerned with achieving some type of behavioural outcome. Only in a relatively few cases did the originator of the message appear to be attempting to evoke in its recipients, any sense of fear, anxiety, dread or danger regarding the likely consequence of the security threat. In other words, while it was not a universal finding, many such messages were devoid of any evidence that the originator carefully selected his or her words for their appropriate connotations, or used symbols known to have an association with such commonly experienced human emotions.

6. Research

Two pilot studies were undertaken. The objective of each study was to establish whether the embedding of a relevant graphic relating to some known aspect of information security, when placed inside an information security message, would have any influence on the information security risk perceptions of any individual to whom the message was being communicated.

To this end, a one-page survey form, containing both a risk message and a semantic differential (SD) grid, was designed for each study. The SD grid was designed to be completed by the message recipient to provide an idea of his or her perception of some of the emotional aspects of the message. By way of explaining the SD grid procedure to the survey respondents in each study, they were provided with a sample grid using the concept/heading Global Warming Debate as the entity or thing to be considered, as shown below.

GLOBAL WARMING DEBATE

			Neutral			
positive	**X**					**negative**
gentle				**X**		**harsh**

Figure 1: Sample semantic differential grid used in each study

The survey form used to generate the results of our first study came in two versions. Version A had no graphic embedded and version B had the graphic embedded behind the complete message. The research subjects (i.e. survey participants) for this first study, were undergraduate students of the University of South Australia. There were two classes of students for this course, each at a different campus. The first class (of 35 students) was given version A of the form, that is, the one without any graphic and the second class (of 40 students) was given version B of the form.

The survey form used in our second study also consisted of two versions. In this instance however, each message contained a graphic. The difference concerned its placement. That is, Version A had a graphic embedded above the salutation of a supposed email message, while Version B had the same graphic embedded following the signature at end of the email message. In this instance, 36 Masters students from the University of South Australia participated.

The objective of the first study was to determine the extent of the emotional impact of an information security message relating to fake emails, i.e. the phishing threat and subsequent risks. The responses between the two groups of students, namely those who got the message without an embedded graphic and those who got the message with an embedded graphic, were compared.

The objective of the second study was to determine the extent of the emotional impact on a message recipient when a graphic associated with the detection of a computer virus was placed either at the beginning of an email message, or at the end of the message.

In both studies, the method of eliciting a response from each participant involved the use of a type of semantic differential (SD) grid. In many instances this procedure has been employed as a method for eliciting attitudinal responses to an issue, item or event. This SD grid consisted of 10 scale items, however, four of these acted as “filler items”. Our main concern was in differences between the student responses to the six scale items meant to elicit reactions in respect to what are known as the Evaluation, Potency and Activity (EPA) dimensions. In general terms, the responses given would give indicate how the participants viewed the security message they were given in terms of its status, power and expressiveness. In more specific terms, the responses were an indication of the extent that each individual student saw the information security message as:

a) good or bad for them
b) strong or weak with respect to them, and
c) as an active or passive thing.

The following figure is a copy of the SD grid used in both studies. For the purposes of this paper, the E-P-A designation for the 3 pairs of relevant scales are is on the left-hand side.

		Extremely	Somewhat	Neutral	Somewhat	Extremely	
A	active						passive
	calm						excitable
P	strong						weak
	relevant						irrelevant
E	beautiful						ugly
A	fast						slow
E	valuable						worthless
	hard						soft
	clever						dull
P	heavy						light

Figure 2: Actual semantic differential grid used in each study

6.1 Research Results

On completing an analysis of the responses to the SD for the first study, no significant differences were detected between the groups with respect to any of the six scales. That is, the data obtained from the respondents who received the phishing message contained within an embedded graphic, in proportionate terms, did not differ significantly from the data obtained from the respondents who received the same message, but without the addition of an embedded graphic. Not surprisingly, when the same procedure was carried out after combining the responses to each of the two scales that made up the Evaluation, Potency and Activity dimensions respectively, again no significant proportionate differences between the two groups was found.

A number of explanations could be put forward to account for these findings. Perhaps the most plausible explanation is that the connotations inherent in the wording of the message were sufficient to get its negative import across - so much so that the graphic provided relatively little by way of additional emotion arousing effects.

As was the case with our first study, on completing an analysis of the responses to the SD for the second study, no statistically significant differences were detected between the groups with respect to any of the six relevant scales. That is, the data obtained from the respondents who received the message with the graphic placed at the beginning, did not differ significantly from the data obtained from the respondents who received the same message, but for whom the graphic appeared at the end. After combining the responses to each of the two scales that made up the

Evaluation, Potency and Activity dimensions respectively, again no significant proportionate differences between the two groups was found.

Although none of the results obtained met the criteria for statistical significance, which is not perhaps surprising given the relatively small sample size, nevertheless it seems that the differences were large enough for the present authors to be convinced that the SD measures used are indeed appropriate for larger and broader purposes.

7. Conclusion

The aim of this paper was, firstly, to discuss how the risk perceptions of computer end-users may be influenced by improving the process of risk communication by embedding symbols and graphics within information security messages. The second aim was to describe some pilot study research that the authors have conducted in an attempt to ascertain whether the embedding of symbols and graphics within information security messages achieves a shift in the risk perceptions of computer end-users.

The authors believe that if the effectiveness of the various forms of risk communication within an organisation can be increased, then the general perception of the risks to the information systems will be more realistic. This is in line with Heiser's (2005) claim that "After political issues, risk perception issues represent the biggest challenge for the security professional. Accurately understanding risk and effectively communicating that understanding to others is core to any risk management role".

There are many ways in which information risk communication could be made more effective. For example, in previous papers and field work the present authors have attempted to show how the concept of "message framing", in line with message recipient's cognitive style could be used. This paper, on the other hand, attempts to show how the use of graphics and symbols could be used to convey risk messages more effectively.

As a final point, it must be emphasized that this paper does not in any way attempt to provide any 'silver-bullet' solutions for management in terms of what they can do towards managing information risk - this was not the aim of this paper. However, it does outline research that is being undertaken by the authors at the time of writing, the ultimate objective of which is to subsequently advise management on how they can communicate information risk simply and more effectively to achieve the final outcome, being the mitigation of actual risks, as shown in Figure 3 below.

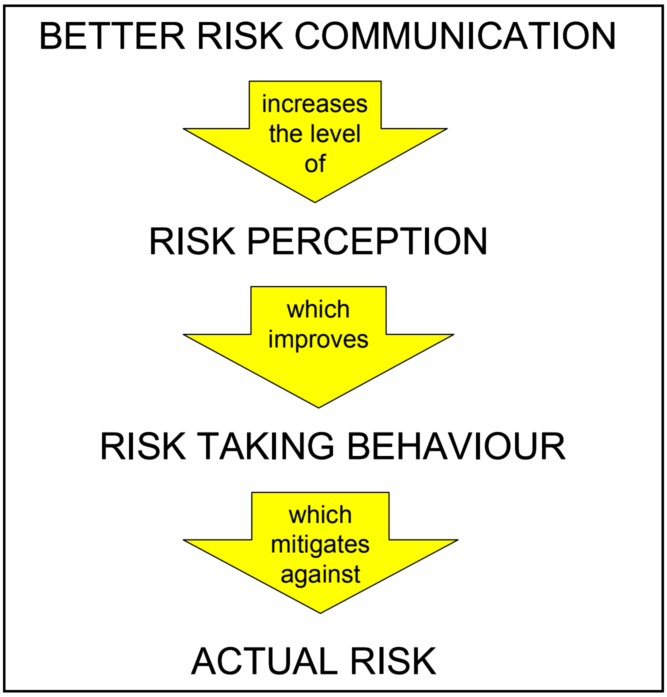

Figure 3: Logical hierarchy of risk outcomes

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.

Bang, M., 1991, *Picture This, How Pictures Work*, Bulfinch Press, Little, Brown and Company.

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.

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

Coleman, J. J., 2005, "Presenting Information on Risks", *Journal of Clinical Pharmacy and Therapeutics*, Vol. 30, pp. 511-514.

HAISA, 2007, "Conference Concept", International Conference on Human Aspects of Information Security and Assurance, Plymouth, UK, July, 2007, Available at http://www.haisa.org/, viewed 12 January, 2007

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

Heiser, J. G., 2005, "Read at your own Risk", *Information Security,* Sept 2005, Layer 8, Tech Target IT Media.

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

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.

OSHA, 1997, *Hazard Communication: A Review of the Science Underpinning the Art of Communication for Health and Safety*, US Department of Labor, Occupational Safety & Health Administration.

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

Pincus, J, D., 2005, "Computer Science is really a Social Science", Microsoft Research, Available at http://research.microsoft.com/users/jpincus/cs%20SocSci.html, viewed 14/01/2007.

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

Schneier, B., 2000, *Secrets & Lies: Digital security in a networked world*, John Wiley & Sons, NY, USA.

USNRC, 1989, *Improving Risk Communication*, National Research Council, Committee on Risk Perception and Communication, Washington, D.C., National Academy Press.

Visual Expert, 2003, "Are Warnings Effective?" Visual Expert Human Factors, Available at http://www.visualexpert.com/Resources/dowarningswork.html, viewed 06/04/2007.