EMPLOYEE SECURITY PERCEPTION IN CULTIVATING INFORMATION SECURITY CULTURE

Omar Zakaria[2]
Information Security Group, Royal Holloway, University of London, Egham, Surrey,TW20 0EX England

Abstract: This paper discusses employee security perception perspective. Perception is important as employee behaviour can be influenced by it. The intention is not to attempt an exhaustive literature review, but to understand the perception concept that can be used to cultivate an information security culture within an organisation. The first part highlights some of the concepts of perception. The second part interprets the employee security perception in the case study. Finally, a synthesized perspective on this perception is presented.

Key words: Information security; information security culture; employee; employee security perception; perception; perception analysis; case study.

1. INTRODUCTION

Schlienger and Teufel (2002) argue that information security culture should support all activities in a way that information security becomes a natural aspect in daily activities of every employee (i.e. user). Ward (2002) explains that the development of information security culture must result in change in employee behaviour. Zakaria and Gani (2003) state that information security culture can lead an employee to act as a "human

[2] He has been awarded a scholarship from the University of Malaya, Kuala Lumpur, Malaysia to pursue his PhD at the Royal Holloway, University of London

firewall" in order to safeguard organisational information assets. This means that employees must perceive security practices as part of their daily work routines. Without appropriate employee security perception, an organisation will stay largely exposed to security threats and vulnerabilities, and later will hinder internal security incidents. Thus, the subsequent sections will discuss concepts of perception and describe how the employee security perception can be used to cultivate security culture within an organisation.

2. CONCEPTS OF PERCEPTION

This section discusses the relationship between perception and behaviour. In general, perception may involve conscious awareness (i.e., this awareness is termed a percept or perceive) of objects, groups, symbols and events, which in turn requires some action on the part of the perceiver (Sekuler and Blake, 1994). Whilst behaviour is about what people normally do (i.e. perform an action) that can be objectively measured (Hogg and Vaughan, 2002). Huczynski and Buchanan (2001: 212) elaborate the perception and behaviour relationships in this statement: "to understand each others' behaviour, we need to be able to understand each others perception. We need to be able to understand why we perceive things differently in the first place". We can see that perception can influence behaviour. In terms of information security context, the right perception can help shape positive security behaviour. Positive security behaviour is about recognising how the theoretical security policies and procedures can be applied into practice. Once employees understand this security behaviour, they will practice it. When these practices are common, it will emerge as part of daily work routine. Later, customised security routines will develop, which in turn produces a culture of information security amongst employees within an organisation.

Over many years, researchers have studied perception for several reasons. Some of these reasons are based on practical considerations in order to solve a particular problem (Sekuler and Blake, 1994). Thus, in the following paragraph, we will provide a brief description on practical reasons for studying perception, which in turn can help us to reduce internal security incident problems.

Through the study of perception, one can recognise and rectify possible risky environmental conditions that can endanger the senses and impair the ability to make decisions (Sekuler and Blake, 1994). In relation to aspects

of information security, security perception of information risk like avoidance and detection controls can help identify potentially internal security incidents (Peltier, 2001). Perception is able to reveal the actual employee basic assumptions about security within an organisation. Any mismatch between these assumptions with official security policies will influence users' perception on security matters. A wrong users' security perception will discourage them to perform security actions. No security actions amongst users will lead to a likelihood of security incidents happening internally (Egan and Mather, 2005). Therefore, through perception, we can predict possible security behaviour.

Furthermore, studying perception enables one to design devices that ascertain optimal perceptual performance (Sekuler and Blake, 1994). Some of these devices are traffic lights, telephones, alarm clocks and car signals in which people rely on during their daily life routine (e.g., during work, communication, driving, even sleep). In relating to information security, recognition of security perception amongst employees can help to design devices like an effective awareness and training programme, design for daily basic security task, even the way to manifest latent function of security mission explicitly.

Studying perception is also useful for consumer marketing (Sekuler and Blake, 1994). For example, companies in the food and beverage industry can test their products by asking consumers to taste, smell or even look at the appearance before marketing them. Therefore, utilising perception research to any products can help bring those products to the attention of customers. In information security context, we can also apply this marketing style to get employee's perception about the security task to be implemented in the organisation. By utilising this approach, we can get the most appropriate and suitable design of basic security task. Once the design is suitable to everyone, employees would be willing to practice it. This design would then become part of the daily work routine.

Therefore, it is important to make sure that the employee security perception is appropriate or suitable, specifically on information security activities. Appropriate or suitable users' security perception means that everyone assumes security activities are part of their daily work routine. Once appropriate security perception is established amongst employees, security actions will be based on their positive security behaviour, which follows the official security policies. Moreover, we have also discussed several ways to use the perception approach in order to improve security practices within an organisation. In summary, Figure 1 shows one of

practical ways to establish an appropriate employee security perception.

In the next two sections, we will discuss the two parts of employee security perception. The beginning part (in section 3) will interpret employee security perception theme in the case study of XYZ Company. Finally (in section 4), we will produce a synthesised perspective on the appropriate employee security perception within a public sector organisation context.

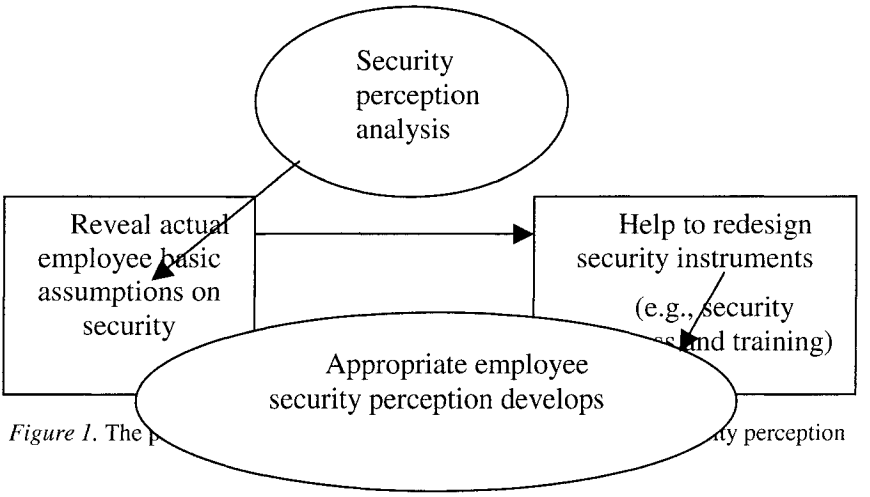

Figure 1. The p ty perception

3. INTERPRETING EMPLOYEE SECURITY PERCEPTION IN THE CASE STUDY

We use the suggested practical way (see Figure 1) for establishing an appropriate employee security perception to interpret the security perception amongst users in the XYZ case study. As discovered in this case study, users in XYZ were already concerned on information security but some of their perception on security tasks was different. Through our analysis of XYZ, employees always claimed that they have a specific Information Communication Technology (ICT) security division within the organisation, which looks after security tasks; their security staff who do the security tasks (e.g., monitor and maintain the security computer system); and their Information Communication Technology Security Officer (ICTSO) person, who does the managing of information security in XYZ. A culture of information security amongst users will not succeed if they are not involved in security activities (Babiak et al., 2005). This is because security activities involve actions which require participation not

only from Information Security Officer (ISO) personnel but also from all users. An established security action will produce repeated security work, which in turn can be a part of daily work routines. Later, a security culture environment amongst users will be developed. Without security activities amongst users, there would be no security actions involved, which could lead to inappropriate security perception which derives from statements such as "Security tasks are not a part of my job" or "I am not responsible for any security matters".

Research in XYZ has shown that information security awareness and training programmes do not fully utilised users' security perception analysis in designing its module. There was no survey done in XYZ in order to know the current security perception amongst users. As already mentioned, perception analysis can be used to design an effective security instruments such as design of basic security tasks and security awareness and training programme. Perception analysis can help to structure basic security tasks properly in order to encourage all users to perform them. This is because these security tasks are designed based upon users' requirement (e.g., result from perception analysis). In short, this analysis can help us to design awareness and training programme based upon users' current security problems. In summary, perception analysis is useful to redesign security instruments and help us to understand users' implicit basic assumptions on security matters.

Therefore, highlighting appropriate security perception in users' basic assumptions should be considered as an emergent activity. Thus, the following section will offer a discussion on a synthesised perspective on the development of an appropriate security perception amongst employees.

4. A SYNTHESISED PERSPECTIVE ON APPROPRIATE EMPLOYEE SECURITY PERCEPTION

It becomes clear from the discussion so far that organisations also need to develop a strategic security vision that ties corporate security plans with the result of the users' security perception analysis. As mentioned above, an appropriate security perception amongst users can influence their security behaviour in order to accomplish the pre-determined security goals. Therefore, it is important to change any inappropriate user perception on security matters. It sounds ideal, but can it operate in practice? The

following paragraphs in this section will discuss examples on changing user perception on security matters positively. Therefore, this section identifies some key principles for developing an appropriate employee security perception.

Principles

There is a general lack of using employee security perception analysis within an organisation and how it influences employee security behaviour which in turn can help interact with users' daily work routines. Therefore, it is essential to link results from the perception analysis and security practices amongst organisational users. This is because appropriate security perception may produce positive employee security behaviour. As a result, users will perform security tasks and assume it as part of the daily work routine. By adopting an appropriate employee security perception, we tend to highlight its practical applications (e.g., redesign security instruments) that can be used in the development of an information security culture. In short, an appropriate security perception amongst employees will help increase security precautions within an organisation, which in turn, can help reduce internal security incidents from happening. In addition, Sekuler and Blake (1994: 8 and 9) emphasises the rational of studying perception and extending its reasons into the development of an appropriate employee security perception as follows:

> Perception can be thought of as each individual's personal theory of reality, a kind of knowledge-gathering process that defines our view of the world. Because this perceptual outlook guides our activities, both mental and behavioural, we naturally find it fascinating to inquire about the bases of perception.

One can see that Sekuler and Blake's statement shows a clear statement about perception which in turn can help redesign any security programmes and instruments for all employees in an organisation. Underlying these redesigning security programmes and restructuring of security instruments is a set of principles which would give an appropriate security perception and assist analysts to develop a culture of information security amongst employees in an organisation. Moreover, these principles could help to reduce internal security incidents from happening. These principles are:

Principle 1: Manifestation of latent function can increase appropriate security perception amongst employees.

One of the ways to increase appropriate security perception amongst employees is using latent function. A manifestation of the latent function (i.e., from implicit form into explicit form) can be used to make everyone in the organisation aware of security matters. This is because the latent function shows clearly how everyone is responsible in the security precautions within an organisation. The latent function is also like a manifest function that can be used to display a security mission. A simple analogy containing a manifest function and a latent function is the data confidentiality. For example, use of a cryptography mechanism as a mean to protect the data from an unauthorised disclosure during transmission, constitutes a manifest function whereas encouraging users to only practice confidential ways when handling their PC constitutes a latent function. Without highlighting latent function to employees like not practising screen saver on computer monitor while not at the workplace could influence the data confidentiality in the computer system and may cause disclosure of secret information in the organisational computer system. Therefore, once everyone understands the latent function, they may perceive security in a more positive manner, which would encourage them to practice security precautions in their daily work routines. In addition, a security awareness programme can be used to highlight this latent function. Thus, this function can become one of the practical ways to increase appropriate security perception amongst employees and later engender security culture effectively.

Principle 2: Security perception analysis can help to redesign security awareness and training programmes and can also encourage appropriate security perception amongst employees.

As mentioned earlier, perception analysis can reveal the employee implicit basic assumption on security matters. From this analysis, we can find out the problems employees had to deal with any security activities, tasks and precautions in their daily work routines. Once we know the problems, we can redesign security awareness and training programmes to educate them. A redesign programme that includes the latest solution for the current security problems may increase positive security perception amongst staff. This is because security awareness presentation is intended to tell individuals about standards, policies, guidelines, procedures, and encourage them to respond accordingly (McLean, 1992). Security training programme will then develop knowledge and skills, which can assist in their security tasks. At the same time, these programmes can promote

security matters, and everyone will be held responsible and requires participation from all staff in security tasks. Once we cope with the latest security problems, we can increase security precautions in the organisation which can lessen internal security incidents from occurring. Thus, figure 2 shows the complete logical hierarchy from Figure 1 to the principles highlighted in section 4 in order to provide a conceptual idea of how an appropriate security perception among staff can be used to develop information security culture.

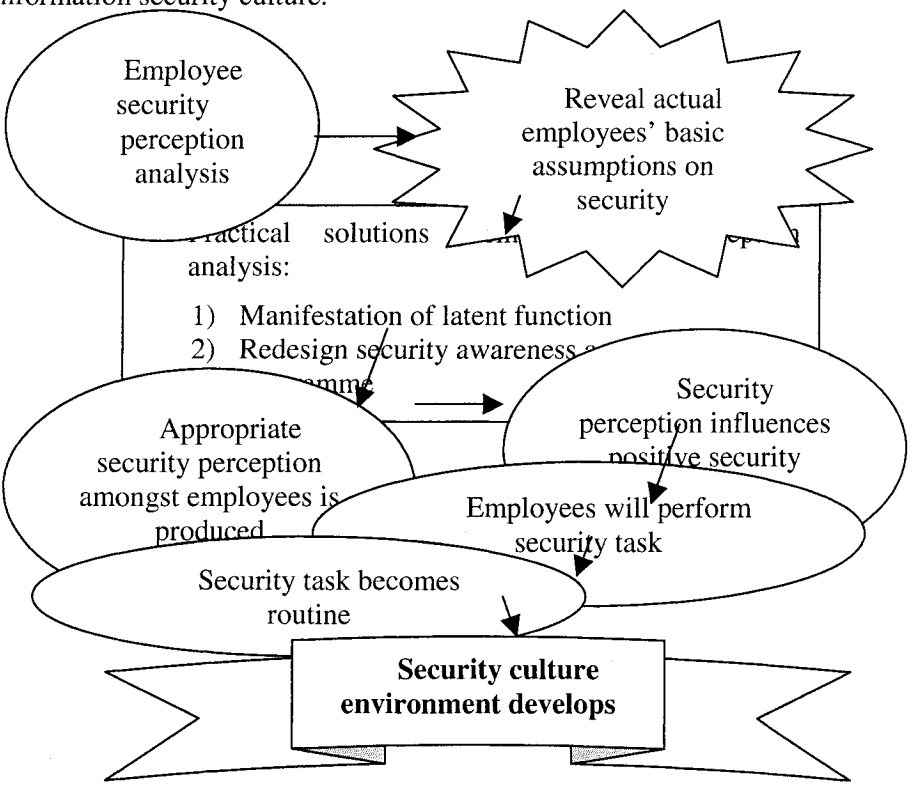

Figure 2. Employee security perception solutions for cultivation of information security culture

5. CONCLUSION

The aim of this section was to highlight the importance of appropriate employee security perception. The basic ideas of

perception and its relevant terms are explained in section 1. It seems clear what an appropriate security perception amongst employee's means in the development of a security culture within an organisation. Through security perception analysis, we are promoting practical principle solutions that can be used to increase appropriate security perception amongst users. An appropriate security perception will influence positive security behaviour, which in turn produce employees who are willing to perform all security practices (e.g., security precautions and security tasks) in their daily work routines. Through these proposed principles, we can also change the current nature of security perception from "they are responsible" to "all of us are responsible" in terms of security practices within an organisation. Moreover, performing security practices by everyone in the organisation can help reduce internal security incidents from happening (Babiak et al., 2005). Therefore, we would like to emphasise that an appropriate employee security perception and its analysis can help increase an organisation's ability to meet information security culture challenges.

REFERENCES

Babiak, J., Butters, J., and Doll, M.W., 2005, Defending the Digital Fontier: Practical Security for Management, John Wiley & Sons Inc, Hoboken, NJ.

Egan, M. and Mather, T., 2005, The Executive Guide to Information Security: Threats, Challenges and Solutions, Pearson Education Inc, Upper Saddle River, NJ.

Hogg, M. A. and Vaughan, G. M., 2002, Social Psychology, 3rd Ed, Prentice Hall, Essex, England.

Huczynski, A. and Buchanan, D., 2001, Organizational Behaviour: An Introductory Text, Prentice Hall Europe.

McLean, K., 1992, Information security awareness – selling the cause, *IT Security: The Need for International Cooperation.* Proceedings of the IFIP TC 11 8th International Conference on Information Security IFIP/Sec'92. North-Holland, Singapore, pp. 179-193.

Peltier, T. R., 2001, Information Security Risk Analysis, Auerbach, Boca Raton, Florida.

Schein, E. H., 1992, Organizational Culture and Leadership, 2nd Ed, Jossey-Bass, San Francisco, CA.

Schlienger, T. and Teufel, S., 2002, Information security culture: the socio-cultural dimension in information security management". In Ghonaimy, M. A., El-Hadidi, M. T. and Asian, H. K. (eds), *Security in the Information Society: Vision & Perspectives*, Kluwer Academic, pp. 193-201.

Sekuler, R. and Blake, R., 1994, Perception, McGraw-Hill, Inc. USA.

Ward, J., 2002, Developing a culture of information security, *Proceeding of the 19th World Conference on Computer Security Audit and Control*, London, pp.193-200.

Zakaria, O. and Gani, A., 2003, A Conceptual Checklist of Information Security Culture, *Proceeding of the 2nd European Conference on Information Warfare and Security*, MCIL, Reading, England, pp. 365-371.