Internalisation of Information Security Culture amongst Employees through Basic Security Knowledge

Omar Zakaria[1]

Information Security Group, Royal Holloway
University of London, Egham, Surrey, TW20 0EX, UK
o.b.zakaria@rhul.ac.uk

Abstract. This paper discusses the concept of basic security knowledge. This concept is about organisational members possessing basic security knowledge that can be applied to perform security tasks in their daily work routine. The intention of this paper is not to attempt an exhaustive literature review, but to understand the concept of basic security knowledge that can be used to cultivate a culture of information security in an organisation. The first part highlights some of the basic ideas on knowledge. The second part interprets the concept of basic security knowledge in the case study. Finally, a synthesised perspective of this concept is presented.

1 Introduction

There is often confusion between the terms – "data", "information" and "knowledge". The term *data* is used to refer to a set of discrete and objective facts about events [3]. In an Information Communication Technology (ICT) system, data is stored in structured records such as a spreadsheet, a database, a log and a document. Data must be sorted and logically coordinated to produce crucial information [4]. Whilst, the term *information* means that manipulated data are crucial for a specific use [4]. The term *knowledge* is about experience, beliefs, norms, concepts or information that can be communicated and shared [1]. In short, information is a result from an analysed data. [2] adds that knowledge is reasoning about information to actively guide task execution, problem solving, and decision making in order to perform, learn and teach. [8] states that characteristics of knowledge are about derives from minds at work, which develop over time, supported by rules, an action-oriented, keep constantly changing, which in turn becomes internalised in the minds of knower.

In organisational context, therefore, knowledge is often imbedded not solely in the documents or even repositories but also in organisational processes, practices, routines and norms. Thus, basic security knowledge can be treated as organisational members able to perform, learn and teach security task in terms of inspection, protection, detection, reaction, and reflection procedures on security matters.

---

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

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

According to [6], there are two types of knowledge – tacit knowledge and explicit knowledge. Tacit knowledge is stored in someone's head, it is not usually internalised and generally lost when the individual resigns or retires. Whilst, explicit knowledge is what that is available to other individuals in whatever form like codified knowledge. Some examples of codified knowledge are reports, best practices, procedures, policies and patents.

[9] elaborate that knowledge is the entire set of insights, procedures and experiences that are considered true, and therefore guide the communications, behaviours and thoughts of people. It sounds ideal, but can we manage knowledge especially security knowledge in practice? According to [5], managing knowledge (i.e., well known as knowledge management) is considered as knowledge creation to an individual process (e.g., tacit knowledge) that can be tranformed into a collective practice (e.g., explicit knowledge). In terms of security context, we can say that managing knowledge can change 'centric responsible', as in operation unit staff to 'collective responsible', such as everyone. This is because through collective practice, everyone in an organisation knows how to perform security tasks, and in turn, creates a collective security responsibility amongst employees. This implies that some security tasks like basic security tasks can be delegated to everyone in the organisation (i.e., this means that we can relate basic security knowledge with basic security tasks).

As already mentioned above, it is essential to change tacit knowledge to explicit knowledge in terms of knowledge creation especially on security knowledge amongst employees in organisations. This is because security knowledge must be externalised in order to share and learn everyone's security practices, which in turn can encourage each employee to perform, learn and teach security tasks effectively and efficiently.

In summary, the combination of everyone's security practices can help the security management people to redesign a better security practice amongst organizational members (see Figure 1).

2 Interpreting Concept of Need to Know Basic Security Knowledge in the Case Study

We use the conceptual idea of basic security knowledge in Figure 1 to interpret the theme of basic security knowledge concept in the ABC company case study. Users in ABC are already concerned with security matters but some of them still do not share their security knowledge in order to overcome current security incidents. Through our analysis in ABC and based on the virus attack in August 2003, some employees managed to perform security tasks based upon the operation unit's instruction and their own experience. However, others did not manage to do it themselves. The reasons were that some subordinates were afraid to teach their superiors how to perform the tasks and others still assume that the security tasks were the operation unit's responsibility.

Research in ABC shows that there were brainstorming sessions, dialogues and discussions conducted in this organisation as a platform to share security knowledge amongst staff. However, not all users came to these sessions to share and learn about security matters. There were the same persons attending almost all these programmes.

Other users assumed that attendance was not compulsory and expected that only technical staff who are ICT-qualified should attend such programmes. It seems that sharing security knowledge is amongst technical staff only and not all users know this knowledge, which might be useful to tackle any security problems during daily work routines. In addition, awareness and training programmes were not solely focusing on ABC's staff participation but the whole Malaysian public sector.

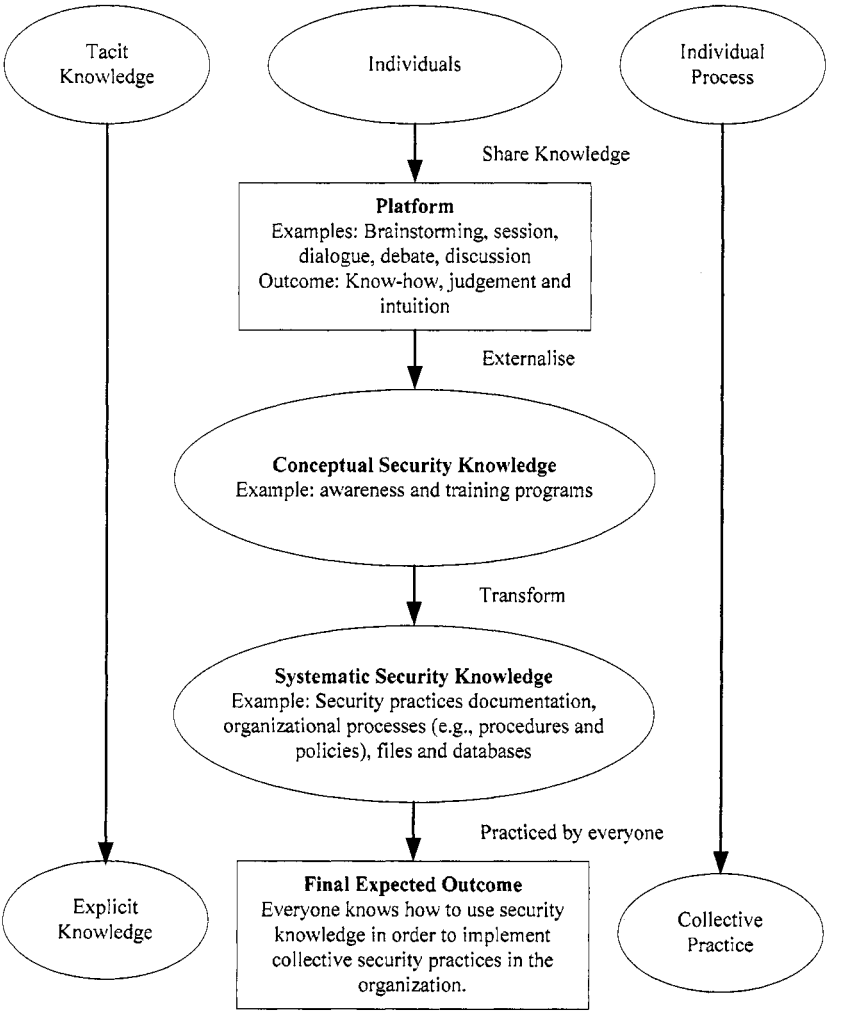

Fig. 1. Externalisation of basic security knowledge in the development of collective security practices in an organisation.

3 A Synthesised Perspective on the Concept of Basic Security Knowledge

It is clear from the discussion so far that organisations also need to develop a strategic vision that ties corporate security plans with the development of basic security knowledge amongst employees. This section identifies some key principles for the manipulation of basic security knowledge concept.

Principles
There is a general lack of knowledge from tacit security knowledge to explicit security knowledge within an organisation and how it interacts with employees' daily work routines. In short, these principles are:

Principle 1: Basic security knowledge should cover fundamental aspects from evaluating current security processes to reviewing incident response procedures.
A basic security task should contain basis aspects from evaluating current security processes to reviewing incident response procedures – inspection, protection, detection, reaction and reflection processes [7].

Principle 2: Participation from all employees in security knowledge sharing sessions.
Through these sessions, they can understand the security problems that everyone in the organisation. Besides this, they can obtain information from others on how to perform certain security tasks.

Principle 3: Good peer relationships can help security knowledge sharing.
Individuals will share information or knowledge to others when they have already established a good relationship with. Therefore, we can relate use this natural way in order to establish a good peer relationship.

Principle 4: Basic security knowledge should include recognition of what is reward and punishment in terms of security matters.
Reward and punishment in terms of security matters are about positive and negative security behaviour. Through the reward and punishment scheme, everyone can differentiate what is honour and penalty.

Principle 5: All basic security knowledge should be documented.
Knowledge should be documented into security practices documentation, procedures and policies.

4 Summary

It seems clear what basic security knowledge means for the development of security culture within an organisation. These proposed principles could also help change security task paradigm from specific individual security processes (i.e., only operation

unit are responsible for security) to collective security practices (everyone is responsible on security).

References

1. Allee, V. (1997), The knowledge revolution: expanding organizational intelligence. Boston, Butterworth-Heinemann.
2. Beckman, T. J. (1997) A methodology for knowledge management. International Association of Science and Technology for Development (IASTED) AI and Soft Computing Conference Banff, Canada.
3. Davenport, T. H. and Prusak, L. (1997). Working knowledge: how organizations manage what they know. Boston, MA, Harvard Business School Press.
4. Gatewood, R. D., Taylor, R. R. and Ferrell, O. C. (1995). Management: comprehension, analysis and application. Chicago, Irwin.
5. Lilley, S., Lighfoot, G., and Amaral, P., (2004), Representing organization: knowledge, management, and the information age, Oxford, UK, Oxford University Press.
6. Nonaka, I. and Takeuchi, H., (1995). The knowledge creating company, New York, Oxford University Press.
7. Pipkin, D L (2000). Information security: protecting the global enterprise. Upper Saddle River, New Jersey, Prentice-Hall.
8. Sveiby, K. E., (1997), The new organizational wealth: managing and measuring knowledge-based assets, San Francisco, CA, Berrett-Koehler Publishers.
9. Van der Spek, R. and Spijkervert, A. (1997). Knowledge management: dealing intelligently with knowledge. In Knowledge management and its integrating elements, Ed by Liebowitz and Wilcox, CRC Press.