Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

A Constructive Approach to Information Systems Security Training: An Action Research Experience

Juhani Heikka
University of Oulu, juhani.heikka@oulu.fi

A Constructive Approach to Information Systems Security Training: An Action Research Experience

Juhani Heikka
University of Oulu
juhani.heikka@oulu.fi

ABSTRACT

Information systems (IS) security breaches cause significant losses to organizations worldwide. Many approaches have been introduced in order to improve employees' security behavior. Earlier research shows that only seven out of 59 approaches are based on sound theoretical background, and the research in the area of IS security awareness and security behavior has neglected the use of relevant theories of psychology, pedagogy and management. The lack of utilizing theories may have a negative impact on the effectiveness of IS security training and on understanding how to change and improve employees' security behavior towards compliance to organizational information security policies. In this paper we describe a theoretically grounded approach to IS security training based on constructivism. The approach is empirically validated in a telecommunications company. The results show that the approach has a positive impact on employees' security behavior.

Keywords

Information systems, security, training, awareness, constructivism.

INTRODUCTION

According to latest studies, information security breaches cause financial losses to the majority of organizations worldwide (Gordon, Loeb, Lucyshyn and Richardson, 2007; DTI, 2007). A significant proportion of these breaches are caused by people not complying with organizational IS security policies. IS security awareness can be defined as a state where employees are aware of and committed to the organization's security mission (Siponen, 2000a). IS security awareness deals with the use of IS security programs to create and maintain security-positive behavior (Kruger and Kearney, 2006). According to Tucker's (2002) report, 44% of 583 organizations worldwide rated their information security awareness level as inadequate. Eyong (2005) came to a similar result, i.e. that IS security awareness among full-time employees is not at acceptable level. The poor situation may be partly explained by the survey with 1,167 respondents from various American organizations, which revealed that 35% of employees had never taken part in any type of security training (Stanton, Stam, Mastrangelo and Jolton, 2005).

Empirical results in different areas (cf., Nelson, Whitener and Philcox, 1995; Puhakainen, 2006) suggest that training plays an important role in assisting an organization to achieve its corporate objectives. Buckley and Caple (1990, p. 13) define training as a planned and systematic effort to modify or develop knowledge, skills or attitude through learning experience, to achieve effective performance, an activity or range of activities. The goal of IS security training is to gain understanding of IS security and modify peoples' security behavior (Layton, 2005). One of the main challenges is that a large part of IS security research has been, and still is, technical in nature, with limited consideration of people and organizational issues (Aytes and Connolly, 2003; Dhillon and Torkzadeh, 2006; Kotulic and Clark, 2004; Siponen, 2000b). While IS security research is moving away from a narrow technical point of view (Dhillon and Backhouse, 2001), human issues, such as improving security behavior or IS security training, have not received enough attention (Siponen, 2000b). According to Siponen (2000a) minimizing human-related errors requires a systematic approach based on behavioral theories. Many researchers have criticized IS security training efforts for their lack of theoretical foundations and psychological eye on changing peoples' security behavior (Björck, 2004; Kabay, 2002; Mattia and Dhillon, 2003; Puhakainen, 2006; Siponen, 2000a, 2000b). In addition, a large proportion of IS security awareness studies are conceptual, lacking empirical validation of their usefulness (Pahnila, Siponen and Mahmood, 2007; Puhakainen, 2006; Siponen, 2000a). This situation may lead to poor training outcomes, which compromises organizational IS security. Organizational IS security solutions may lose their effectiveness if employees do not follow IS security policies and instructions.

The findings above suggest that there is a clear need for theoretically grounded, empirically validated approaches to improve IS security awareness within organizations. In this paper we describe a theoretically grounded approach to IS awareness training based on constructivism. The approach is empirically validated in a Finnish telecommunications company through action research.

The paper is organized as follows: section two includes a review of related work. The third section describes the research methods and settings. The fourth section provides the results of IS security training. The fifth section discusses the results, and the last section includes the conclusions.

RELATED WORK

According to Siponen (2000b), Peltier (2005) and McIlwraith (2006), the most commonly used approaches aimed at minimizing human-related faults are IS security awareness, education and training. These approaches aim at increasing employees' intentions to comply with organizations' information security policy and the use of security solutions (Siponen, 2000b). The point of departure for IS security awareness is to create an IS security policy and instructions that describe how security should be addressed in the organization. The problem is that people do not always follow the IS security policies or safe practices (Aytes and Connolly 2003; Stanton et al., 2005). It is a well-known fact that IS policies alone do not have an impact on employees' security behavior (Albrechtsen, 2007; Wood, 1997). Researchers have suggested the use of IS security campaigns (in the form of using mass emails, posters and merchandise promoting security) in order to improve IS security behavior among employees (e.g., Desman, 2002; Herold, 2005; McLean, 1992). While some researchers see the campaigns as good measures for improving attitudes, Siponen (2000a) points out that poor planning of campaigns may lead to unwanted results in terms of motivation, attitudes and negative feelings. In addition, campaigns are not efficient in changing peoples' actual behavior. For example, the study by Albrechtsen (2007) showed that employees did not even remember the IS security campaign carried out in a company, and that it had no impact on their security behavior. In the analysis of the results Albrechtsen (2007) found supporting arguments from safety psychology arguing that pure information seldom has any effect on individual behavior, as behavior is created by more factors besides knowledge and attitudes (cf., Aytes and Connolly, 2003; Layton, 2005; Pahnila et al., 2007).

Many researchers and practitioners suggest training as a mean for improving IS security awareness within organizations (e.g., Desman, 2002; Furnel, Gennatou and Dowland, 2002; Herold, 2005; Katsikas, 2000; McIlwraith, 2006; Peltier, 2005; Roper, Grau and Fisher, 2006). IS security awareness training usually aims at two main goals: gaining knowledge or awareness of existing security threats and developing skills to apply proper countermeasures (Aytes and Connolly, 2003). Prior research indicates that only few of the IS security awareness training programs take into account important factors such as motivation, attitudes and beliefs affecting security behavior (cf., Marcinkowski and Stanton, 2003; Siponen, 2000a, 2000b). According to Kabay (2002), such factors as peoples' beliefs, attitudes and behavior on individual and group level must be changed in order to improve IS security in organizations. In addition, Mattia and Dhillon (2003) argue that IS security research is unable to make much progress without integration of social and behavioral areas, such as motivation, cognition and organizational learning.

The major challenge of different IS security awareness approaches is the lack of use of theoretical background and empirical validation of the suggested approaches. Puhakainen (2006) analyzed 59 IS security awareness approaches represented by IS security researchers and practitioners. The results of the analysis illustrate that only seven out of 59 IS security awareness approaches provided a theoretical background. Further, the results show that the majority of studies focus on conceptual analyses without empirical validation of approach (53 of 59 studies). The empirical results by Puhakainen (2006) show that employees' security behavior can be changed through systematic IS security training based on relevant behavioral and learning theories. The results above show that there is a clear need for theoretically grounded IS security training approaches that are validated through field study. Empirical validation is important in demonstrating the effectiveness of the suggested approach, and field studies have also been called for by researchers (Puhakainen, 2006; Siponen, 2000a, 2000b; Yngström, 1996).

RESEARCH METHODS AND SETTINGS

Research methods

The empirical part of the study was carried out as action research (AR). Common characteristics of AR include action and change orientation, a problem focus, and an organic process involving systematic stages that are carried out in collaboration among participants. AR has also been described as a technique characterized by intervention experiments that operate on specified problems perceived by practitioners in a particular context. In practice, AR aims simultaneously at two goals: (1) to produce new scientific knowledge by putting theories to work and (2) to solve the practical problem in the participating organization. (Baskerville, 1999.) In AR, the researcher is concerned with creating organizational change in collaboration with subjects, and simultaneously with studying the process (Baskerville & Myers, 2004). By merging research and practice AR produces highly relevant research results and it has been proven useful in the context of IS and organizational studies (cf., Burnes, 1993; Puhakainen, 2006; Siponen, Baskerville and Heikka, 2006).

AR intervention consists of five phases (Figure 1). The research environment includes rules under which the researcher and practitioners agree on the boundaries and actions of the research domain. The first phase, *diagnosis*, aims at identifying problems that are the underlying causes of the organization's desire for change. In *action planning*, the different alternatives for problem solving are considered in collaboration with the researcher and practitioners. This phase specifies organizational actions that should relieve the problems identified. The discovery of planned actions is guided by the theoretical framework that indicates some desired future state for the organization. In *action taking*, the researcher and practitioners collaborate to carry out the planned actions causing certain changes in the organization. After the field intervention, the results are *evaluated* to find out whether the problems were solved. Evaluation also includes determining whether the theoretical effects of the action were realized. *Specifying learning* includes the identification of the general findings of the study that provides important knowledge to the scientific community. The findings can be also used as a base for future AR interventions. (Baskerville, 1999.) Surveys, interviews, observations and field notes can be utilized in data collection (Baskerville and Wood-Harper, 1996).

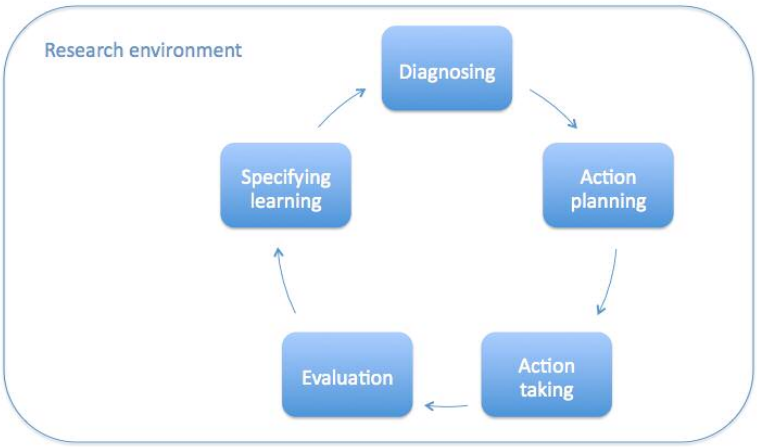

Figure 1. The five-step action research cycle (Baskerville 1999).

Research settings

The case company operates in the telecommunication sector providing broadband, cable TV and mobile phone services. The company employs about 250 persons working in three business units: marketing, information systems and administration services. According to the company's IS security manager, the telecommunication sector is under constant change and the company is developing new business models and services that require a high level of information security. The telecommunication sector is regulated by the Finnish Communications Regulatory Authority, which defines the IS security regulations and statutes that the company must comply with. The company had earlier carried out a monitoring of employees' PCs that revealed unauthorized material from several employees' computer. The company's IS security manager had also observed several neglections of the company's IS security policies (e.g., writing down passwords and neglect of managerial responsibilities). The acts of neglect had resulted security breaches such as stealing of a company laptop and personal belongings from the office. For this reason, the company was an ideal environment for testing the IS security training approach and its effectiveness in improving employees' security behavior.

In order to improve the IS security practices in the company and to solve the organizational problems, collaboration between different stakeholders was required. As indicated in the literature review, there is a clear need for empirical IS security studies. According to Baskerville and Wood-Harper (1996), the discipline of IS seems to be a very appropriate field for the use of AR, and studies have been called for by IS security scholars (cf., Baskerville and Myers, 2004; Dhillon and Backhouse, 2001). For these reasons AR seemed to be an advantageous research approach for our purposes.

IMPLEMENTING THE ACTION RESEARCH IN THE COMPANY

In the ***diagnosis phase*** our research team interviewed 32 of the company's employees from different business units between October 2005 and February 2006. The interviews were recorded and the results were reported to the company's representatives. The purpose of the interviews was to gain knowledge about IS security challenges existing in the company and to recognize relevant targets for improvement. Several interviewees reported that managements' attitude towards IS security should be improved and that the IS security organization of the company should be strengthened. An employee reported as follows: *"The general atmosphere and my supervisors' attitude could be improved – if the supervisor does not set*

a great store by information security, consequently the subordinates do not care about it". Other employee put it as follows: *"There is a need for management support for IS security activities…the situation used to be better earlier when we had more security resources"*. Because the company had been obliged to cut resources, the role of middle management in maintaining IS security was emphasized. Next, a field survey (cf., Pahnila *et al.*, 2007) was carried out that was answered by 86 of the company's employees (response rate 35%). The data were analyzed and the findings supported the results of the interviews and observations made by the company's IS security manager. The survey implicated three main targets for improvement: (1) middle management's role in maintaining information security, (2) visibility of security in the company and (3) compliance with the company's security policies.

In the beginning of ***action planning***, we arranged a meeting where we discussed the diagnosis findings with the company's IS security manager and Human Resource Management (HRM) Chief. They agreed that there is a need for IS security training that would help the company to emphasize reasons for complying IS security policies and to improve target groups' security behavior. In designing and implementing IS security training we applied the systematic approach to training of Buckley and Caple (1990, p. 26–34). First, we carried out knowledge, skills and attitudes analysis, decided the target population and the training needs. Prior to this research, the company had arranged a few informative IS security awareness meetings in the auditorium supported with computer-based IS security training that was compulsory for the staff, and over 95% of the company's employees completed these. These two activities formed a baseline for the IS security training. The company's IS security manager, HRM chief and Systems Specialist decided that the middle management would be a perfect target group for training for several reasons. *First*, the middle management is responsible for communicating IS security related topics to their subordinates. *Second*, they are also responsible for supervising that subordinates comply with the company's security policies. *Third*, subordinates reported in the survey and interviews that they need more support from their managers in order to follow the company's IS security policies. *Finally*, the IS security managers saw the potential that middle management could pass the message to their subordinates (cf. cascade training in Buckley and Caple, 1990). The company's representatives listed the most crucial topics that the training should cover. The topics included the most important IS security responsibilities of the middle management, the recent security breaches in the company and the observed neglect of the company's IS security policies.

Next, we considered learning principles and training methods. Earlier studies and experiences suggested that constructivism would also be a fruitful approach for IS security training because it helps to activate the participants and their thinking. Constructivism, a psychological theory of learning, stems form a dynamic field of cognitive science, based on the initial work of Jean Piaget and Lev Vygotsky. The theory is based on models of evolution and development. It construes learning as an interpretative, recursive, nonlinear building process by learners interacting with the surrounding physical and social world. Teachers practicing constructive approach reject the notion that meaning can be passed on to learners via symbols and transmission. This means that learners cannot incorporate exact copies of the teacher's knowledge for their own use. Instead, the constructivist view of learning emphasizes the opportunity for concrete and contextually meaningful experience through which the learners can search for patterns. (von Glasersfeld, 2005.) Although constructivism is not a theory of teaching, it suggests taking a radically different approach to instruction from that utilized traditionally in teaching (Phillips, 1995). For example, in behaviorism learners are viewed as passive subjects in need of external motivation or reinforcement. In contrast, a constructivist view of learning necessitates (a) involving learners actively in their learning by suggesting an approach to teaching that gives (b) learners the opportunity for concrete, contextually meaningful experience through which the learners can raise questions, interpret the knowledge and defend their strategies and ideas. From a constructivist perspective the (c) role of the teacher is not to teach in the traditional sense of delivering instruction to a group of learners. Rather, they (d) use materials that activate learners (cognition) to get them involved through (e) social manipulation or interaction (reflective abstraction). Constructivism also (f) emphasizes the idea of an integrated curriculum where learners study the topic in various ways, for example by reading material about the topic, discussing the topic, learning new vocabulary related to the topic and through hands-on experience in real-world exercises. (Fosnot and Perry, 2005.) These six perspectives of constructivism steered the designing and implementation of the IS security training in the company. The training methods selected and material created were piloted in a meeting with the company's IS security manager and HRM chief, leading to minor adjustments of the vocabulary used in the material and removal of some less relevant subtopics.

After action planning, IS security training of the middle managers was carried out in the ***action taking phase*** in April 2007. 29 of company's middle managers attended the training that was implemented as an interactive lecture promoting social interaction (discussions) on the topics and exercises. The goal of the training was to improve managers' security behavior, to highlight their security responsibilities and to pass the message to their subordinates (cascade training). The training consisted of three main sections. *First,* we discussed the topical information breaches, such as stealing of a laptop computer and removal of old employees' user accounts, which had taken place recently in the company. This worked as motivation for learning new knowledge and constructing a meaning to comply with the company's IS security policies. *Second*, we

discussed the most important managerial security responsibilities and the topics recognized by the company's IS security manager and Systems Specialist. Next, we went through the means that managers can apply in order to affect their subordinates' security behavior. The last part of the training consisted of discussing the findings of the interviews and the survey. This part of the training allowed the managers to reflect the results on their own actions and enabled their opinions to become visible. They did a small group exercise where they had to recognize the most valuable assets that are crucial for their work and think how they ensure the information security of that asset. At the end of the session, the managers were given homework to think how they would improve the visibility of information security in the company and how they would improve information security among their subordinates.

THE IMPACT OF THE TRAINING ON MANAGERS' SECURITY BEHAVIOR

The impact of the information security training was ***evaluated*** by utilizing semi-structured interviews. We sent an interview invitation to all 29 managers who participated in the training. Some managers said that they were too busy and some did not want to participate in interviews for various reasons. 12 managers volunteered for interviews that were recorded and transcribed (one manager did not want the interview to be recorded and it was documented by making exact field notes). The length of the reflective interviews varied from 40 to 90 minutes, being on average about 60 minutes. The material started to saturate around the tenth interview, so we stopped the interviews after those that had already been booked. In this paper the interviewed managers are identified in the quotations by indexing them from M1 to M12.

The interviews had two purposes: (1) to measure the effects of the training on managers' security behavior and (2) to reflect the new knowledge in relation to their group and work tasks. Common ways to assess learning include direct observations, written and oral responses and self-reports. In this study, learning is assessed through self-reports which are learners' statements and ratings of themselves that can take in various forms like interviews, think-alouds and dialogs (Schunk, 2000). In the interviews three managers reported that the training did not change their security behavior. A manager working in IS maintenance reported as follows: *"The training did not change my behavior a lot because the behavior has been on adequate level."* (M1). According to another experienced manager *"The training did not have an impact on my security behavior. I have been working in this field for decades so I know information security issues pretty well"* (M9). The quotations above indicate that some managers may find it difficult to question their behavior, although it is important as new kinds of IS security threats arise all the time.

Changes in Operations Models and Security Attitudes

The majority of the managers interviewed reported that the IS security training had a positive impact on their security behavior, and several managers had questioned their current ways of working. For example, one manager reflected in the interview as follows: *"I have arranged team meetings regularly for 15 years… Now I realized that I have had a section for every other thing except information security, which is an important part of our service production. There is a clear need for changing our operation model, and information security will be added to our team meetings' agenda, there's no doubt about it."* (M7). According to another manager: *"There were things [in the training] that surprised me. I had imagined that security things are in better shape."* (M2). Another manager reported that the message is now passed on to his subordinates: *"The factual content [of the training] was very important and it is certain that I will discuss these things with my subordinates"* (M3). Passing on the message to subordinates (cascade training) was one of the goals of training and it was mentioned in seven interviews. In addition, controlling of office was mentioned in the interviews. According to one manager: *"The training did wake me up to control my own office."* (M8). The company's IS security policy defines that guests should be taken to meeting rooms instead of own offices because there are usually documents in the offices that are for internal use only.

Behavioral Changes in PC Use

Several managers reported that they started to lock their computers after the training. As one manager put it: "*Before the training I did not lock my computer even though it was easy. I have started to lock my computer systematically after the training – now I always lock my laptop. I changed the settings in such a way that when I close the lid the laptop locks itself."* (M6). A manager working regularly outside the company office reported that *"the training reinforced that when I am outside our office on customers' premises, I make sure that the laptop is at all times visible to me and if I have to go somewhere during that time I will certainly lock the doors."* (M8).

Conflict of Interest

One interesting finding that arose in the interviews was the paradoxical role of managers and specialists. According to a "specialist manager" their role is exceptional: *"People working in a special area are different, they are professionals and*

everyone perceives information security as daily routines that do not need extra attention" (M4). The assumption that professionals do not need surveillance may be hazardous, as shown by many examples from history (e.g., Enron, Société Générale, cf. Willison, 2004). Another manager also saw the role of surveillant as problematic: *"The concept of information security must go top-down, but managerial work is still often seen as secondary and people will rather act as specialists in technology. In a manager's shoes you have to monitor others and lead others to comply with instructions. Who else would do that – it is the manager's job."* (M5). Even though these things were discussed in the IS security training, it seems that changes in specialist's and surveillant's roles go much deeper in the organization culture. The change requires more effort in the future.

DISCUSSION

The results of this study show that it is beneficial to apply learning theories in designing and implementation of IS security training, as has previously been suggested by many researchers (e.g., Kabay, 2002; Siponen, 2000a; Puhakainen, 2006). By applying the systematic approach of Buckley and Caple (1990) and constructivism (Fosnot and Perry, 2005), we were able to develop an IS security training that had a positive impact on managers' security behavior, attitudes and working practices. The empirical results indicate that emphasizing the key mechanisms of constructivism (cf., (a)–(f) above) in IS security training enables learning and improving employees' security behavior (cf., Fosnot and Perry, 2005, p.34).

The results of this study support the earlier findings that constructivist learning theories are useful in the context of IS security awareness (cf., Puhakainen, 2006). However, this study provides a wider spectrum of behavioral changes that are important in changing the security behavior among a company's employees. A positive finding was that the approach supported the idea of cascade training (Buckley and Caple, 1990), which can be applied in the case of larger organizations where it is impossible to train every single employee.

The empirical results also indicate that in some cases the training did not have an impact on managers' security behavior. One possible explanation is that change would have required longer duration of the training. Changing organizational culture, including roles, values and norms, is usually a longer, organization-wide change process that takes years (Burnes, 1993). Another possible explanation is conflict of interest. The results presented here indicate that managers are more interested in working as specialists than surveillants of security behavior of subordinates, which causes a conflict of interest. Similarly, the study by Albrechtsen (2007) reported that complying with security policies increases the workload, which may cause a conflict between security and efficiency. A third possible explanation is that the managers should have been divided into smaller groups (less than ten persons) as suggested in the analysis by Puhakainen (2006).

The study does not come without limitations. The findings presented in this paper are based on one organization. In order to improve the generalizability of the results more research and empirical results from various industries are needed. In the case of AR, generalization is problematic, because an intervention in a unique organizational setting can never be repeated (Baskerville and Wood-Harper, 1996). In addition, assessing learning is difficult because we do not observe it directly, but rather its products and outcomes (Schunk, 2000). For that reason, someone may question the reliability of self-reported changes in security behavior when the trainer and interviewer are the same person. There are some efforts to create objective tools for measuring the impact of IS security trainings on employees' security behavior (cf., Kruger and Kearney, 2006), but the area is still largely ignored by research (Puhakainen, 2006).

Baskerville and Wood-Harper (1998) have proposed validity criteria for information systems AR that were applied in this study: (1) the research was set in a multivariate social situation; (2) the observations were recorded and analyzed within an interpretive frame; (3) researchers' actions intervened in the research settings; (4) the method of data collection included participatory observation; (5) changes in the social setting were studied; (6) the immediate problems in the social setting were resolved during the research and (7) the research illuminates a theoretical framework which explains how the actions led to a favorable outcome.

CONCLUSIONS

Information security and IS security awareness are great challenges for researchers and practitioners. Earlier studies had recognized the lack of use of theories and empirical validation of the IS security awareness approaches developed. In this study we described theoretically grounded IS security training, which was validated through action research. The results implicate that by applying constructivism in the context of IS security training, the security behavior of employees can be improved. The study provided new scientific knowledge about changing people's security behavior. It also provided a practical approach to IS security training. The described training approach may be useful for persons responsible for improving employees' security behavior within an organization. Further research is needed to improve the approach described here and to expand the approach to concern the entire organization and also in other fields.

REFERENCES

1. Albrechtsen, E. (2007) "A Qualitative Study of User's View on Information Security," *Computer & Security* 26, 276–289.
2. Aytes, K. and Connolly, T. (2003) "A Research Model for Investigating Human Behavior Related to Computer Security," *The Proceedings of the 9th Americas Conference on Information Systems*, 2027–2031.
3. Baskerville, R. (1999) "Investigating Information Systems with Action Research," *Communications of the Association for Information Systems* 2, Article 19.
4. Baskerville, R. and Myers, M.D. (2004) "Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice – Foreword," *MIS Quarterly* 28 (3), September 2004, 329–335.
5. Baskerville, R. and Wood-Harper, T. (1996) "A Critical Perspective on Action Research as a Method for Information Systems Research," *Journal of Information Technology* 11, 235–246.
6. Baskerville, R. and Wood-Harper, T. (1998) "Diversity In Information Systems Action Research Methods," *European Journal of Information Systems* 7, 90–107.
7. Björck, F. (2004) "Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations," *Proceedings of the 37th Hawaii International Conference on System Sciences*, 70186b.
8. Buckley, R. and Caple, J. (1990) Theory and Practice of Training. Kogan-Page Ltd, London.
9. Burnes, B. (1993) Managing Change: A Strategic Approach to Organisational Development and Renewal. Pitman Publishing, London.
10. Department of Trade and Industry (DTI) (2007). "Information Security Breach Survey 2006," Department of Trade and Industry Publications, UK.
11. Desman, M.B. (2002) Building an Information Security Awareness Training Program. Auerbach Publications, London.
12. Dhillon, G. and Backhouse, J. (2001) "Current Directions in IS Security Research: Toward Socio-Organizational Perspectives," *Information Systems Journal* 11 (2), 127–153.
13. Dhillon, G. and Torkzadeh, G. (2006) "Value-focused Assessment of Information Security in Organizations," *Information Systems Journal* 16, 293–314.
14. Eyong, K.B. (2005) "Information Security Awareness Status of Full Time Employees," *The Business Review* 3 (2), 219–226.
15. Fosnot C.T. and Perry R.S. (2005) "Constructivism: A Psychological Theory of Learning" in Constructivism: Theory, Perspectives and Practice. 2nd edition. Ed. Fosnot, C.T. Teachers College Press, London.
16. Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002) "A Prototype Tool For Information Security Awareness and Training," *Logistics Information Management* 15 (5), pp. 352–357.
17. Gordon L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. (2007) "2006 CSI/FBI Computer Crime and Security Survey," Computer Security Institute Publications.
18. Herold, R. (2005) Managing an Information Security and Privacy Awareness and Training Program. Auerbach Publications.
19. Kabay, M.E. (2002) "Using Social Psychology to Implement Security Policies," in Bosworth, S. and Kabay, M.E. (editors), *Computer Security Handbook*, 4th edition, John Wiley & Sons, USA.
20. Katsikas, S.K. (2000) "Health Care Management and Information Systems Security: Awareness, Training or Education," *International Journal of Medical Informatics* 60, 129–135.
21. Kotulic, A.G. and Clark, J.G. (2004) "Why There Aren't More Information Security Research Studies," *Information & Management* 41, 597–607.
22. Kruger, H.A. and Kearney, W.D. (2006) "A Prototype for Assessing Information Security Awareness," *Computers & Security* 25, 289–296.
23. Layton, T.P. (2005) Information Security Awareness: The Psychology Behind the Technology. AuthorHouse, USA.
24. Marcinkowski, S.J. and Stanton, J.M. (2003) "Motivational Aspect of Information Security Policies," *The Proceedings of the IEEE Systems, Man, and Cybernetics Conference*, 2527–2532.

25. McIlwraith, A. (2006) Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness. Gower Publishing Limited, England.
26. McLean, K. (1992) "Information Security Awareness – Selling the Cause," *Proceedings of the IFIP TC11*, 1–11.
27. Nelson, R.R., Whitener, E.M. and Philcox, H.H. (1995) "The Assessment of End-User Training Needs," *Communications of the ACM* 37 (7), 27–39.
28. Pahnila, S, Siponen, M. and Mahmood, A.M. (2007) "Employees' Behavior Towards IS Security Policy Compliance," *Proceedings of the 40th Hawaii International Conference on System Sciences*, 156b.
29. Peltier, T.R. (2005) "Implementing an Information Security Awareness Program," *EDPACS (The EDP Audit, Control and Security Newsletter)* 33 (1), 1–19.
30. Phillips, D.C. (1995) "The Good, the Bad, and the Ugly: The Many Faces of Constructivism," *Educational Researcher* 24 (7), 5–12.
31. Puhakainen, P. (2006) "A Design Theory for Information Security Awareness," *Acta Universitatis Ouluensis Scientiae*, Rerum Naturalium, A 463. Available at http://herkules.oulu.fi/isbn9514281144/
32. Roper, C.A., Grau, J.A. and Fisher, L.F. (2006) Security Education, Awareness and Training: From Theory to Practice. Elsevier Butterworth-Heinemann, Oxford, UK.
33. Schunk, D.H. (2000) Learning Theories: An Educational Perspective, 3rd edition. Prentice-Hall, USA.
34. Siponen, M. (2000a) "A Conceptual Foundation for Organizational IS Security Awareness," *Information Management & Computer Security* 8 (1), 31–41.
35. Siponen, M. (2000b) "Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice," *Information Management & Computer Security* 8 (5), 197–202.
36. Siponen, M., Baskerville, R. and Heikka, J. (2006) "A Design Theory for Secure Information Systems Design Method," *Journal of the Association for Information Systems* 7 (11), 725–770.
37. Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005) "Analysis of End User Security Behaviors," *Computers & Security* 24, 124–133.
38. Tucker, T. (2002) Security Awareness Report Index: The State of Security Awareness among Organizations Worldwide. PentaSafe Publications.
39. Von Glasersfeld, E. (2005) "Introduction: Aspects of Constructivism," in Constructivism: Theory, Perspectives and Practice. 2nd edition. Ed. Fosnot, C.T. Teachers College Press, London.
40. Willison, R.A. (2004) "Understanding the Offender / Environment Dynamic for Computer Crimes: Assessing the Feasibility of Applying Criminological Theory to the IS Security Context," *Proceedings of the 37th Hawaii International Conference on Systems Sciences*, 1–10.
41. Wood, C.C. (1997) "Policies Alone Do Not Constitute a Sufficient Awareness Effort," *Computer Fraud & Security*, December 1997, 14–19.
42. Yngström, L. (1996) "Security Training and Education for IT Professionals," *International Journal of Bio-Medical Computing* 43, 105–113.