MIS Quarterly

RESEARCH ARTICLE

IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY[1]

By: **Petri Puhakainen**
IS Security Research Center
Department of Information Processing Science
University of Oulu
Oulu
FINLAND
petri.puhakainen@oulu.fi

Mikko Siponen
IS Security Research Center
Department of Information Processing Science
University of Oulu
Oulu
FINLAND
mikko.siponen@oulu.fi

Abstract

Employee noncompliance with information systems security policies is a key concern for organizations. If users do not comply with IS security policies, security solutions lose their efficacy. Of the different IS security policy compliance approaches, training is the most commonly suggested in the literature. Yet, few of the existing studies about training to promote IS policy compliance utilize theory to explain what learning principles affect user compliance with IS security policies, or offer empirical evidence of their practical effectiveness. Consequently, there is a need for IS security training approaches that are theory-based and empirically evaluated. Accordingly, we propose a training program based on two theories: the universal constructive instructional theory and the elaboration likelihood model. We then validate the training program for IS security policy compliance training through an action research project. The action research intervention suggests that the theory-based training achieved positive results and was practical to deploy. Moreover, the intervention suggests that information security training should utilize contents and methods that activate and motivate the learners to systematic cognitive processing of information they receive during the training. In addition, the action research study made clear that a continuous communication process was also required to improve user IS security policy compliance. The findings of this study offer new insights for scholars and practitioners involved in IS security policy compliance.

Keywords: IS security, IS security training, employees' compliance with security policies

Introduction

User noncompliance with IS security policies[2] is increasingly cited as a key IS security problem in organizations (CSI/FBI

[1]Detmar Straub was the accepting senior editor for this paper. Suprateek Sarker served as the associate editor.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

[2]IS security policy documents are called by various names in different organizations. Further, multiple types of security policy documents may exist at different levels in a single organization, such as documents for high-level IS security strategies and more granular, operational-level guidelines (Baskerville and Siponen 2001; Dhillon 1997). In this paper, we refer to the latter as IS security policies.

Computer Crime and Security Survey 2007). If users do not comply with IS security policies, IS security measures lose their efficacy (Backhouse and Dhillon 2001; Straub and Welke 1998). To address this concern, a number of approaches have been advanced in the literature, including the use of sanctions based on deterrence theory (Siponen et al. 2007; Straub 1990), marketing campaigns (McLean 1992) and training and education (Siponen 2000a). Sanction-based approaches argue that fear of sanctions determines whether employees comply with the policies (Akers and Sellers 1994; Straub 1990; Siponen et al. 2007). In contrast, the reputed aim of IS security policy training and education is to persuade employees and activate employees' thinking processes. In this way, employees internalize the reasons why it is important to comply with security policies (Gardner 2004). Sanctions reportedly diminish computer abuse (Straub 1990) and increase employee compliance with security policies (Siponen et al. 2007).

In spite of the persuasiveness of punitive approaches, more than 1,000 studies on Cognitive Moral Development in more than 40 countries suggest that non-punitive strategies, particularly cognitive education and training, can be even more effective in justifying compliance with the rules for certain types of people (Rest 1994). In addition, Arvey and Ivancevich (1980) reported that sanctions may work better as a deterrent if they are rationalized and justified through cognitive education and persuasion. Thus, it is no surprise that a variety of IS security training approaches have been suggested in the IS security literature (Puhakainen 2006; Siponen 2000a).

Unfortunately, IS security training and education approaches for compliance have largely remained atheoretical and anecdotal: only four studies are theory-based, and only two provide empirical evidence of their practical efficiency (Puhakainen 2006). We argue that underlying theory and empirical evidence constitutes the cornerstones of IS security training approaches. While philosophers of science from Feyerabend (1964) to Popper (1968), Lakatos (1970), and Laudan (1984) agree that theories are the basis of science, there are also practical reasons why theories are important. Senge et al. (1994) argue that if tools, such as training programs, have no underlying theory, then practitioners acquire tools that might work in one situation but do not know why they ultimately work. Such tools might fail in other situations, but again, the practitioners won't know why. If one doesn't understand the underlying theory behind the tool, then one cannot understand its limitations (Senge et al. 1994).

Hence, mature IS security training programs should provide a theoretical explanation for how and why the programs work. Empirical evidence is similarly important as it indicates whether the training and education approach works in practice, which is the ultimate goal of training. A training program that does not work in practice is of limited value. As a consequence, IS security practitioners need empirically proven approaches to improve compliance in fact. To overcome this deficiency, this study developed an IS security training program that is theoretically and empirically grounded. Action research was conducted to validate and refine the program.

The rest of this study is organized as follows. The next section reviews existing IS security training approaches. A theoretically based IS security policy compliance training program is then developed. The practical usefulness of the program is then validated by testing it through action research. The action research method is discussed, and the action research intervention to implement an IS security policy compliance training program at an organization is described. The implications for research and practice are discussed, followed by a summarization of the findings.

Existing IS Security Policy Compliance Approaches and the Need for a New Approach

Information systems security training studies found in the literature typically incorporate a pedagogical orientation as a primary means of improving user compliance with IS security policies (Table 1). These approaches involved an instructor-led stepwise method, the use of videos (Lafleur 1992; Mitnick 2002; Murray 1991; Peltier 2000, 2002), screen savers (Rudolph et al. 2002), and Web-based tutorials. Of these, only two are theoretically grounded, providing a theoretical explanation of how and why the training program should work. Table 1 summarizes the extant IS security training studies. The "Basis of Findings" column indicates whether the findings of the study are based on informal observations, experiment, case studies, action research, survey or practical experiences, or argumentation. If a theory of education is used, "theoretical orientation of the training" indicates that the training approach is based on behaviorism, cognitivism, or constructivism, also called paradigms of learning (Hung 2001; Karjalainen 2009). The use of any empirical research method, including field experiments, case studies, action research, field-based interpretivist studies, and surveys (see Galliers 1992), is tallied as fulfilling the criterion of empirical evidence. "A" and "P" refer to an academic or practitioner-oriented study, respectively. For a detailed review of these studies, see Puhakainen (2006).

Table 1. A Review of the IS Security Training Literature

Study	Key Findings	Basis of Findings	Academic/ Practical	Underlying Theory and Theoretical Orientation of the Training	Emp. Evidence
Cox, Connolly and Currall (2001)	Suggests a Web-based tutorial and checklist for increasing compliance in academic environments.	Practical experience	**A**	–	–
Desman (2002)	Offers a four-stage awareness program for improving users' security behavior: (1) discovering the current situation, (2) establishing a baseline: developing the program (e.g., documentation, procedures, processes, training), (3) communications (raising the IS security awareness of the organization and motivating employees to follow IS security documentation), and (4) evaluating and updating the awareness program.	Practical experience	**P**	–	–
Goodhue and Straub (1991)	Presents a model of managerial perceptions of systems risk, including IS security training	Quantitative survey	**A**	Theory of Information Quality; behaviorism	**X**
Hadland (1998)	Suggests that training include drama; in addition, leaflets should be used as supportive material.	Practical experience	**P**	–	–
Kajava and Siponen (1997)	Offers a process for maximization of users' compliance especially in a university context.	Practical experience	**A**	–	–
Lafleur (1992)	Suggests an IS security awareness program with two components: (1) a promotional component (publications, advertising, and reaction to incidents) to introduce employees to, remind them of, and induce them to respond to security and (2) an interactive component (briefings, planning sessions, meetings, and training) to achieve improvements in employees' security behavior.	Practical experience		–	–
Mitnick (2002)	Argues for an ongoing IS security awareness training program as a means of influencing people to change their behavior. Suggests the following means to deliver the training: role-playing, reviewing media reports of recent attacks on other companies and discussing how those companies could have avoided the attacks, or showing a security video.	Practical experience	**P**	–	–
Murray (1991)	Suggests the program should be a combination of courses, seminars, videos, handouts, directives, reminders and newsletters.	Practical experience	**P**	–	–
NIST (1996)	Suggests the following seven-step approach for developing an IS security awareness training program: (1) identify program scope, goals and objectives, (2) identify training staff, (3) identify target audiences, (4) motivate management and employees, (5) administer the program, (6) maintain the program, and (7) evaluate the program.	Practical experience	**P**	–	–
NIST (1998)	Proposes three fundamental training content categories: (1) knowledge of laws and regulations, (2) security program, and (3) system life cycle security. An employee's training needs in each of the three areas are determined by his functional specialties as defined by his organizational role.	Practical experience	**P**	–	–

Table 1. A Review of the IS Security Training Literature (Continued)

Study	Key Findings	Basis of Findings	Academic/ Practical	Underlying Theory and Theoretical Orientation of the Training	Emp. Evidence
Peltier (2000, 2002)	Suggests the following means to convey the awareness message: training sessions, books, videos, brochures, newsletters, booklets, and practice with the help of an instructor.	Practical experience	**P**	–	–
Perry (1985)	Suggests the following means to impact user behavior: senior officer attending an IS security seminar, hiring a consultant to review the organization's IS security program, highlighting IS security violations, adding IS security reviews to internal and external audit missions, issuing an IS security policy, and introducing a reward system.	Practical experience	**P**	–	–
Rudolph, Warshawsky and Numkin (2002)	Proposes several techniques for delivering the training: logos, themes, images, lectures with stories and examples, screen savers, sign-on messages, posters, videos, trinkets and giveaways, newsletters, IS security surveys, contests, IS security audits, various events, briefings, conferences, and presentations.	Practical experience	**P**	–	–
Siponen (2000a)	Presents a framework for persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions.	Conceptual analysis	**A**	Intrinsic Motivation, Emotivism	–
Siponen (2000b)	Proposes ethical education to improve employees' IS security behavior, where ethical principles are used to justify claims that certain IS security acts are morally favored.	Conceptual analysis	**A**	Theory of Justice	–
Spurling (1995)	The importance of IS security to the employees should be emphasized through presentations and training, work instructions, e-mail messages, booklets, newsletters and screen savers.	Practical experience	**P**	–	–
Straub and Welke (1998)	Emphasizes IS security awareness training as a means for improving employees' compliance with security policies. Major reason for IS security training is to communicate severity and certainty of sanctions to the employees and review IS security policies.	Action Research	**A**	Deterrence Theory; behaviorism	**X**
Telders (1991)	Users' IS security behavior can be developed and implemented through the following five-step IS security awareness program: (1) researching the environment, (2) designing a security awareness plan, (3) selecting the target audience and designing specific methods for each major exposure area, (4) reviewing and approving the plan by management, and (5) ensuring enough time and other resources to support the security awareness effort on an ongoing basis.	Practical experience	**P**	–	–
Thomson and von Solms (1997)	Identifies three different target groups for such a security compliance program: top management, information systems management and end-users. The following means should be used to deliver the program: presentations, workshops, and continuing material such as booklets, newsletters, multi-media packages, e-mail reminders and screen savers.	Practical experience	**A**	–	–

Table 1. A Review of the IS Security Training Literature (Continued)

Study	Key Findings	Basis of Findings	Academic/ Practical	Underlying Theory and Theoretical Orientation of the Training	Emp. Evidence
Thomson and von Solms (1998)	Proposes a number of rules of thumb to improve the practical efficiency of IS security awareness training.	Literature analysis	**A**	–	–
Tudor (2001)	Presents a ten-phase security training program: (1) develop and schedule training targeted at executive level management, (2) assess security policies, procedures and guidelines, (3) identify strategic information sources and mission critical systems, (4) establish a security awareness and training program committee, (5) review and recommend security tools, (6) establish emergency as well as incident response and reporting procedures, (7) schedule training, (8) identify communication methods, (9) determine security awareness promotional activities, and (10) integrate security into organizational processes.	Practical experience	**A**	–	–
Vroom and von Solms (2002)	Proposes an IS security awareness program with the following steps: (1) educating top management about the necessity of IS security awareness, (2) making use of the existing international IS security standards as a guideline for the IS security policies, (3) creating the IS security policies of the company, (4) reviewing and maintaining IS security, (5) implementing a formal program for IS security awareness, (6) addressing general security measures applicable to all users, and (7) providing guidelines on the protective measures within various departments.	Practical experience	**A**	–	–
Wood (2002)	Stresses the need for a security education campaign.	Practical experience	**P**	–	–

As we can see from Table 1, only two of the previous studies on IS security training provide empirical evidence of their usefulness in practice. In their seminal studies, Goodhue and Straub (1991) and Straub and Welke (1998) emphasize IS security awareness training as a means for improving employees' compliance with security policies. To be more precise, a key objective of IS security training is to communicate sanctions for noncompliance by the employees and review IS security policies for employees. Their approaches are based on behaviorism in terms of the paradigms of learning (Karjalainen 2009). Behaviorist training methods emphasize instruction-led teaching with one-way interaction, the specification of measurable and observable behavioral objectives and quantitative measurement, and the use of reinforcement to gain the learning outcomes (Hung 2001; Karjalainen 2009).

An alternative pedagogical paradigm is constructivism, stressing the interactive, two-way communication between the learners, activating the learners' own thinking processes, and critical reflection of learners' own knowledge and interpretive and conversational forms of evaluation (Hung 2001; Karjalainen 2009). Training approaches based on constructivism are seen as preferred approaches for educating white-collar employees in organizations (Karjalainen 2009). Consequently, there is a need for constructionist IS security training programs that are based on appropriate underlying theories and that offer empirical evidence of their practical usefulness.

To design a theoretically and empirically grounded method for developing constructionist IS security training programs, we next propose a theory-based program for IS security policy compliance training.

Theoretical Framework for Developing IS Security Policy Compliance Training Programs

In seeking candidate theories on which to base the constructionist IS security training program, we proffer education-related theories that meet the two requirements discussed in the previous section. The first requirement is that the IS security training programs provide a theoretical explanation of how and why the training program works. This means that the training program must provide necessary information to the educators, so the educators know the theory of how the training program helps people learn (Clark 2003). In the case of IS security training, the underlying theories should not only explain how people learn, but also what learning principles are expected to change user compliance with IS security policies. Knowing these learning principles helps educators get people to learn, and helps them tailor the training approaches to different organizations and target groups (Clark 2003). As a second requirement, the underlying theory should provide guidelines for how successful training is to be delivered in practice. This is important for practitioners, who need practical guidance on implementing efficient training.

Regarding the first requirement of how and why the training program is expected to work, previous research has demonstrated that cognitive processing of persuasive information is necessary for long-lasting behavioral changes (Gardner 2004; Greenwald 1968; McGuire 1968). However, instead of cognitive processing, the recipient could rely on a variety of cues to make quicker decisions than would be the case if he engaged in detailed cognitive processing. Petty and Cacioppo (1981a, 1986) assert that cues are non-argument elements of the message that can influence a change in attitude without actively thinking about the issue. Hence, cues allow the recipient to adopt an attitude without having to deeply analyze the issue under consideration. Examples of cues are speaker credibility, the reactions of others, external rewards and the attractiveness of the speaker.

Changes as a result of relying on cues are short-lived and unpredictable, whereas changes as a result of the cognitive processing of persuasive arguments are more predictable and persistent (Petty and Cacioppo 1981a, 1986). Consequently, as our goal was to develop a training program with a long-lasting impact on behavior, we need to rely on cognitive processing and at the same time understand the need to avoid cues.

Of the possible theories, the elaboration likelihood model (ELM) has predicted attitude change in the fields of consumer research and marketing (Petty and Cacioppo 1981b, 1984). It explains how predictable, long-lasting behavioral changes can be achieved through cognitive processing. At the same time, it points out that short-lived changes can be avoided by not relying on cues. Consequently, the ELM helps practitioners to understand how and why training is expected to work (requirement 1). Hence, it became our focus as a primary underlying theory for IS policy compliance training.

Regarding the second requirement (how efficient training is to be constructed and delivered in practice), there are several theories guiding the design process for goal-oriented training. Instructional design theories seem to be ideal candidates on which to base our design process for a cognitive IS security training program, since the aim of instructional design theories is to give concrete guidance on the process of developing and implementing goal-oriented instruction. However, instructional design theories (e.g., Dick and Carey 1996; Gagné 1985; Glaser 1971) are typically very general and give little guidance on how to customize training for various environments and target groups. Such general theories are not adequate for our purposes. However, one instructional design theory—the universal constructive instructional theory (UCIT) (Schott and Driscoll 1997)—provides a framework for designing instruction that is customized for a certain learning subject (e.g., compliance with e-mail policy) and target group (e.g., a certain organization, business unit, department, or group). Consequently, UCIT is selected as the second underlying theory base for IS security compliance training.

UCIT and ELM complement each other. UCIT puts forward a concrete framework for developing situated IS security policy compliance training. However, it does not give concrete guidance on selecting suitable training methods for individual target groups. To this end, other theories must be used. For this reason, ELM was selected to complement UCIT. Further, the selection of complementing theories is not guided or restricted by UCIT. These two theories are described in more detail in the next section.

Elaboration Likelihood Model (ELM)

As previously mentioned, changes resulting from reliance on cues (following the peripheral route) are unpredictable, whereas changes resulting from the cognitive processing of persuasive arguments (following the central route) are more predictable and persistent (Petty and Cacioppo 1981a). Consequently, IS security policy compliance training should use training methods that enable the systematic cognitive processing of information.

Petty and Cacioppo (1981a, 1986) argue that motivation is a necessary prerequisite for cognitive processing. A highly motivated recipient is likely to use cognitive processing, whereas low motivation leads to reliance on cues. Petty and Cacioppo recognize that the personal relevance of the topic has a strong impact on motivation. Consequently, when the aim is to motivate cognitive—and avoid superficial—processing of information, IS security policy compliance training should use learning tasks that are personally relevant to the learners.

Universal Constructive Instructional Theory (UCIT)

UCIT guides the training design process via the following four-phase framework (Schott and Driscoll 1997): (1) determination of the instructional task, (2) diagnosis of current state of the learner, (3) constructing and delivering instruction, and (4) diagnosis of success (Figure 1).

Applying UCIT's design process, determination of the instructional task is the first phase. In the context of this study, the instructional task relates to users' compliance with IS security policies. In the second phase, diagnosis of the current state of the learners in relation to the instructional task is explored. Some of the knowledge required for compliance with IS security policies is already known by IS users, but some of the knowledge has yet to be learned. The difference between the knowledge that is required for compliance and the users' current knowledge defines what it is the users still have to learn. This is called the learning task.

In the third phase of UCIT, constructing and delivering instruction, the learning task and the learning environment are constructed and the instruction delivered. In this stage, the aim is to find key issues for efficient design of the situational IS security training (i.e., tailored to fit the organization's specific needs). The instructor should consider only those aspects that are constraints on users' IS security policy compliance in this particular target group (Schott and Driscoll 1997). ELM is used in the third stage of UCIT. Its principles regarding cognitive processing of information give guidance on developing instruction that aims to deliver long-lasting behavioral change in learners. In the fourth phase, diagnosis of success, the success of the instruction is assessed by verifying to what degree users' IS security policy compliance has been achieved.

In addition to these four phases of instruction, UCIT highlights crucial elements for the design and delivery of instruction. They are (1) functions,(2) basic components of instructions,and (3) situated possibilities and constraints for learning in a certain organization (Schott and Driscoll 1997). The functions of UCIT are related to knowledge and have an impact on IS users' learning. These functions are (1) acquisition of knowledge, (2) storage of knowledge, and (3) use of knowledge. The basic components of instruction include (1) the learning environment (including the instructor, teaching methods and media), (2) the learning task (compliance with IS security policies), (3) the learners, and (4) the place in which the instruction takes place.

Of the aforementioned basic components and functions, the learner and his acquisition of new knowledge form the core of learning. Consequently, the design and delivery of our IS security policy compliance training program focused on the learners' efficient acquisition of new knowledge. Finally, UCIT suggests that what will be learned by the learners is influenced by the possibilities and constraints arising out of the learners' previous knowledge. Hence, IS security policy compliance training should leverage the learners' existing knowledge of IS security policy compliance.

Research Approach to Validate the IS Security Training Program in Practice

Research Method

Action research stands out as an ideal research method for validating and possibly refining the IS security policy compliance training program. Owing to the principle of cyclical field intervention, action research allows theory refinement in practice, in addition to theory testing (Baskerville 1999; Baskerville and Wood-Harper 1998). Action research is also a clinical method, aimed at creating organizational change and solving practical problems through the research (Baskerville and Myers 2004). As our aim was not only to validate and possibly refine the IS security policy compliance program in practice, but also to study how the program can be used to change employee behavior, action research seems the perfect method. This is supported by Walsham (2006), who regards action research as the ideal way to perform involved research, where the researcher has direct involvement in the change action in an organization.

Information Collection and Analysis

Three methods were used to collect the research data: (1) interviews, (2) a survey, and (3) participatory observation (see Walsham 2006). Following Walsham, at the beginning of the intervention, an anonymous and open survey (Appendix A) was used to collect information related to employees'

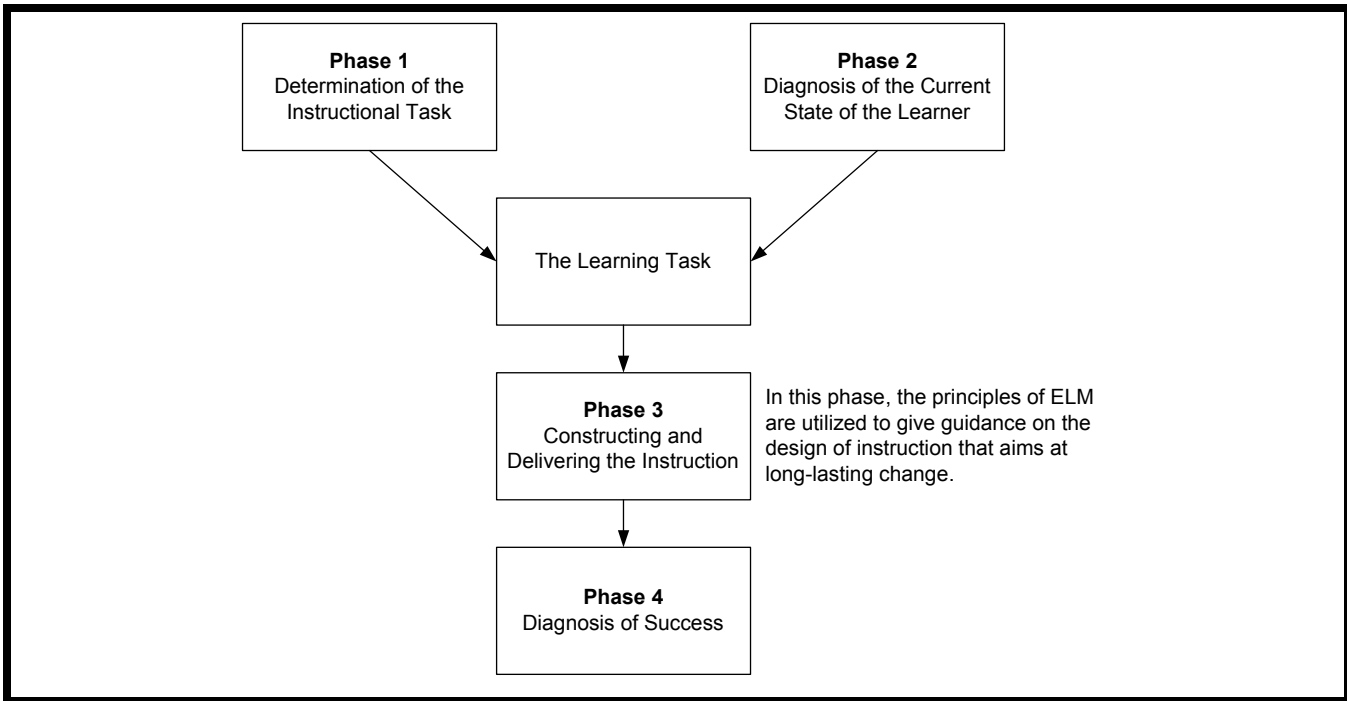

Figure 1. UCIT's Four Phases of Instruction (adapted from Schott and Driscoll 1997, p. 162)

skills regarding, and knowledge of, the secure use of e-mail. The survey was used to ensure anonymity, which in turn ensures that the respondents provide honest answers (Myers and Newman 2007; Walsham 2006). The survey included open questions about information classification rules and the secure use of the Internet and e-mail. This information was used to evaluate whether the employees had the necessary knowledge to comply with the e-mail policy.

In addition to the survey, semi-structured interviews were used to gather information about employee skills, attitude, and knowledge related to compliance with the e-mail policy, especially regarding their current habits, and ability to utilize information classification rules and encryption software (Appendix B). During the analysis phase, the researchers classified the interview data in order to find all of the problems regarding employee compliance with the e-mail policy. In addition, interviews were used to evaluate the results of the intervention. Hence, interviews were carried out before and after the training intervention to determine the effect of the IS security training.

The interviews were conducted with individual employees, but group interviews were also used. Myers and Newman (2007) advise scholars to avoid a situation where only certain selected groups of people are interviewed, resulting in an incomplete presentation of views in the organization. To avoid this issue, all employees were interviewed in normal social interactions and formal interviews. In addition, the anonymous survey was sent to every employee.

All information collected during the interviews was recorded by means of field notes. Initially, the researchers considered using audiotape to record the interviews. This seemed to be the most useful method to avoid follow-up questions and show respect for people's time. However, despite these advantages, the use of an audio recorder was abandoned to make the participants feel more comfortable and relaxed and thus more willing to voice their own opinions and perceptions. This is consistent with Walsham and with Mårtensson and Lee (2004), who reported that the use of tape recorders makes interviewees less truthful and less open. Whenever any doubts about the meaning of an interviewee's statements arose, they were clarified immediately during the interview. Additional clarifications were made during the analysis phase to avoid misinterpretation.

Finally, participatory observation concerning the impact of the intervention was conducted in normal working situations (Walsham 2006). In addition to the researcher, the company's IS security manager and other employees observed the results achieved throughout the study (the security manger and other employees were not part of the formal research team). In this study, each employee was considered an active processor of

the information. Consequently, an employee was regarded as able to decide personally whether to comply with the company's e-mail policy. Additionally, this decision was thought to be affected by his or her social environment. It was not expected that the policy would be obeyed without its reasonableness being questioned. Hence, this study assumes a relativist ontology, meaning multiple realities are socially constructed by the employees (Guba and Lincoln 1989).

Empirical Validation of the Program for IS Security Policy Compliance Training

Background and Participants

The host company, hereinafter referred to as SC, was established in 1997. It is located in Helsinki, Finland. It develops applications for electronic information processing. The company's XML-based products are designed for building cross-organizational processes and services online. This includes the life cycle of information, from its creation to long-term archiving. The action research was conducted with all employees of SC, 16 people altogether, and took place over an 11-month period from August 2004 to June 2005.

The management of the company consisted of three people: a CEO, a marketing director, and a sales director. All three were part of the company's sales team (see Table 2). The sales team also included a sales manager. SC's technical team consisted of five software developers, three technical specialists responsible for customer installation projects, and one employee responsible for testing. Other employees were a sales assistant, an IS security manager, and a legal advisor.

The CEO owned the majority of the stock. Additionally, he was the only formally defined superior in the company and, thus, was responsible for economic and administrative decisions. The technical team was responsible for most product development issues. The IS security manager was responsible for security issues.

Two years before this action research process began, an IS security development program was implemented at SC. As a result of the program, the company's IS security management system was certified according to a valued international information security standard, BS7799 (see von Solms 1999). Consequently, an IS security policy and end-user instructions were already in place, and users had been trained in the procedures before this study commenced. Hence, the management of the company and the researcher could assume a high level of employee awareness of IS security issues.

Although the company was certified by the BS7799 standard and had a program of security training, the IS security manager saw violations of information security policies and procedures, especially the e-mail policy. The e-mail policy states that users should assess the criticality of information in their e-mail messages and take the necessary precautions before sending the e-mail. The only exception to this rule was that it was acceptable to send confidential information unencrypted if the other communicating party (e.g., business partner or customer) was unable to use e-mail encryption. While the option of sending unencrypted e-mail was intended for exceptional occasions only, the IS security manager saw it as the prevailing practice, especially by the sales team members. He saw that this practice risked revealing valuable and confidential information, and that the situation needed to be corrected.

> *I have noticed that employees have sent confidential information by e-mail without encrypting it. I have been told that this is a common way of acting in the sales team. The technical people are more aware of the possible risks. Consequently, I believe that they should encrypt confidential information more often.*

Given this problem, the action research intervention aimed at improving compliance with the company's e-mail policy with the assistance of a training program.

Conducting the Action Research Study at SC

In order to test and refine a theory (Baskerville 1999), the 11-month action research consisted of two research cycles (see Figure 2). The first research cycle at SC involved the implementation of an IS security training program. The first cycle lasted from the middle of August until the end of November. The second research cycle was theory refinement, in which a new communication process was added to make the IS security training program more effective. The second cycle started in December and ended in June.

The First Action Research Cycle

The first research cycle at SC involved the implementation of a training program to increase compliance with the company's e-mail policy. In accordance with action research principles, the training program was executed in the following four phases: (1) identifying the problem, (2) planning the training, (3) delivering the training, and (4) evaluating the results.

Identifying the problem. In the first phase of the first action research cycle, the most critical issues regarding the host or-

Table 2. Employee Tags Used for Anonymity

Group of Users	Number of Users in the Group	ID Tags
Sales team members (CEO, marketing director, sales director, and sales manager	4	st1–st4
Software developers	5	sd1–sd5
Technical specialists	4	ts1–ts4
Other users	3	o1, o2, and IS Security Manager

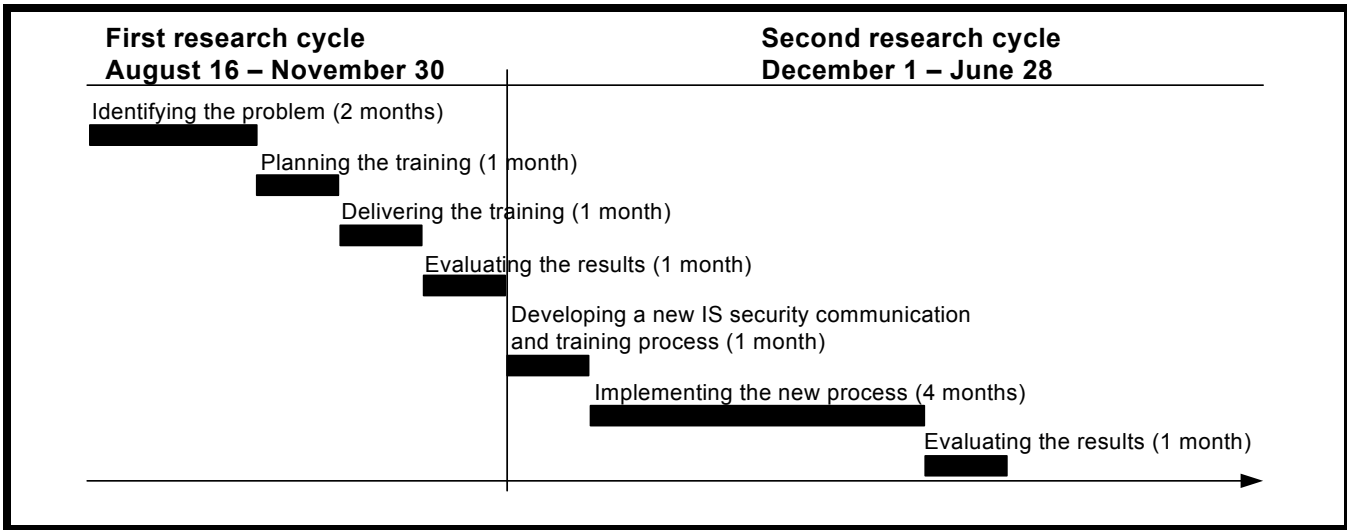

Figure 2. The Time Line of the Action Research Project

ganization's e-mail policy compliance were identified. An anonymous survey (Appendix A) was used to explore to what extent the users were (1) aware of the existence of IS security policies and IS security risks, (2) able to apply the e-mail policy and information classification rules in practice, and (3) aware of and able to use e-mail encryption. In addition to the survey (N = 16), all 16 employees were interviewed. To guarantee their anonymity in the manuscript (Myers and Newman 2007; Walsham 2006;), each employee was assigned an anonymous ID tag (Table 2). The IS security manager did not want to maintain his anonymity, and he is referred to as "IS security manager."

The survey revealed that the users were aware of the company's e-mail policy. While the technical staff was able to use encryption, other employees lacked the skills to encrypt e-mails. The interviews revealed these employees to be three members of the sales team and one person belonging to the group of other users. Moreover, the survey pointed out that the purpose of the information classification rules was recognized, but their use in practice was unclear to four employees, including a software developer who stated,

> *The information classification rules are somewhat unclear. I find it difficult to decide when encryption is really required.*

In the interviews, six employees argued that the instructions were not always followed by management, which lessened the employees' motivation to comply with the instructions.

> *Management seems to be busy with business issues other than security, and they are too often noncompliant with the IS security instructions. This gives the impression that our management does not consider IS security important. This has a negative impact on our motivation to comply with the instructions.* (A software developer)

In the interviews, five employees criticized the usefulness, clarity, accessibility, and format (MS Word document) of the security manual, including the e-mail policy. These five

employees also found the instructions too bureaucratic and verbose, with a lot of technical details.

> *Our security manual should be easier to access. And employees should be reminded more often about the existence of the manual. The instructions in the manual are mainly useful and possible to comply with. However, some of them are too wordy. Consequently, the main idea is difficult to find. A short abstract that summarizes the essence could be added at the beginning of each instruction. This might address this shortcoming. Also, the format of the manual is impractical. An HTML document would be easier to access than an MS Word document.* (A software developer)

> *The security manual contains too much technical jargon, which makes it difficult to understand. Some of the procedures in the manual hinder our getting on with our work. So people sometimes violate the official procedures. However, even in these cases we act in a way that we consider secure enough. I even think that our own procedures are better than the ones described in the manual.* (A software developer)

The responses to the survey revealed that the encryption software used to protect e-mail was seen as easy to use and useful. However, the interviews revealed that sometimes the receiving party didn't have the capability to use the encryption method dictated by the company's IS security instructions (i.e., S/MIME). This was reported by four employees. This had eroded the use of e-mail encryption. For instance, one of the technicians claimed that

> *Often the receiving party has no means to encrypt and decrypt e-mail using S/MIME. In these cases, S/MIME encryption is not useful for our purposes.*

The interviews revealed that four employees felt that work overload, hurrying, suddenly emerging situations and unplanned assignments hindered their compliance with the e-mail policy. Additionally, these four claimed that the receiver's inability to encrypt and decrypt e-mails was one reason for their insecure use of e-mail.

> *Sometimes management and salesmen give us unusual, unplanned, and urgent assignments. This makes us too busy even to think about IS security—not to mention complying with the IS security instructions.* (A technical specialist)

Finally, the interviews pointed out that the sales team did not encrypt its e-mail.

> *A lot of our team's e-mail messages contain sensitive information. However, I suspect that about 90 percent of these e-mails are sent unencrypted. Part of this is caused by the whole team's lack of skills in using e-mail encryption.* (A sales team member)

The problems regarding noncompliance with the e-mail policy are summarized in Table 3.

Planning the training. After the problems were identified, the next phase of the first action research cycle was planning the training. As presented earlier, the learner's acquisition of knowledge forms the core of learning. Consequently, planning the training focused on the learners' efficient acquisition of knowledge. This was to be achieved through training methods that enable learners' cognitive processing of information and give them the motivation to do it.

In terms of UCIT (see Figure 1), this action research phase included determination of the instructional task (first phase of UCIT) and diagnosis of the current state of the learners' (the employees of SC) knowledge regarding the instructional task (second phase of UCIT). In addition, this action research phase included constructing and delivering instruction in terms of UCIT (see the third phase of UCIT in Figure 1). The instructional task (determination of the instructional task in Figure 1) was defined as increasing users' compliance with the e-mail policy. In this particular case, it meant increasing the use of encryption for confidential e-mail. Achieving this required user skill and knowledge.

First, users needed to be aware of the existence of the e-mail policy and understand its content. In particular, they should know the rules regarding the encryption of confidential information. Second, without sufficient knowledge of the company's information classification rules, users would not be able to recognize confidential information. Third, the users should have the skills to use the e-mail encryption software. The difference between the aforementioned skills and knowledge and the users' current skills and knowledge defined the learning task: what the users still needed to learn. To discover this difference, the users' current situation was explored. According to the problem identification phase, the users were aware of the e-mail policy and its contents. However, the information classification principles were unclear to four users and hence required review.

Furthermore, the phase of identifying the problem (the first stage of the action research, Figure 2) indicated that the sales team used e-mail in communicating with customers and partners, and the messages contained confidential information. Despite this, encryption was not used owing to a lack of skill in using e-mail encryption. The technical staff used e-mail

Table 3. Reasons for Violations of the E-Mail Policy at SC

Problems	Source	Planned Solution
Format the content of the e-mail policy	sd1, sd2, sd3, ts1, ts2	Revising SC's security manual (including e-mail policy) before the training program
Perceived lack of management's active example	sd1, sd2, sd3, ts1, ts2, o2	Personal persuasive discussions with the CEO
Technical problems	st1, ts1, ts2, sd1	Seeking alternative encryption methods during the training program
Lack of skills and knowledge	st2, st4	Training program
Work overload and hurry	sd2, sd3, ts1, st4	Was not to be addressed by the action research intervention

encryption more often, and all were able to use it. Hence, it was decided that two separate sets of training sessions with different aims and content would be designed: one for technical staff and one for all other users. Thus, the learning task in terms of UCIT for the training program was decided as follows: The first task was to enable the users to apply the company's information classification rules in practice. The second task was to help the nontechnical users gain the skills necessary to use e-mail encryption (Table 4).

Plan for the first session: The first training session was designed for all users. It had three parts. The first part was designed in the form of a collaborative, instructor-led discussion about the risks related to the use of e-mail. The aim of such a design was to activate the learners' existing knowledge of the subject matter. This was expected to enhance learning, as according to UCIT, learners' prior knowledge has a strong impact on their learning (Schott and Driscoll 1997). In addition, activating learners' prior knowledge enhances their cognitive processing of new information (Clark 2003). Moreover, according to ELM (see Petty and Cacioppo 1981a, 1986), cognitive processing is necessary for long-lasting change.

The second part was designed to use e-mailed documents that had been sent to partners and customers. The goal of such a design was to use the learners' own authentic documents to make the instruction personally relevant to the learners and hence motivate their cognitive processing. The first task was designed for the learners to analyze their documents and find confidential information in them. This was meant to apply the information classification rules and to activate the learners' cognitive processing.

The next task was designed for the learners to analyze possible consequences for the company, the team, and the learners themselves if confidential information was revealed, for example, to competitors. The confidential information included product pricing, development costs of the product and profit, and technical details of the company's own products. For example, leaking of the company's product and pricing information to competitors could result in the company losing ground to its competitors. This would result in significant economic losses for the company. The goal of this task was to make the subject matter significant to the learner and others, which in turn should motivate learners' cognitive processing. Furthermore, the task was designed to build a cause-and-effect mental model. This motivates the learners' cognitive processing, which, according to ELM, is the key to long-lasting change. Finally, it was planned that instant feedback from the instructor be provided to support learning results.

Plan for the second session: This session was designed for nontechnical users. The aim of the session was to enable these users to use encryption software called 7zip. When 7zip is used, the password that protects the encrypted file needs to be shared among all communicating parties. Hence, in addition to the use of the application, the sender must share the password with each receiver through an alternative communication channel, such as the telephone. As this was a new procedure, the instructors expected most users to be unfamiliar with 7zip. Hence, the learning task for the first part was designed for the learners to gain the knowledge and skills required to use 7zip to encrypt e-mails.

Plan for the third session: The third session was designed to review the issues covered in the first two sessions: information classification principles, reasons for encrypting sensitive electronic information, and the use of 7zip for encryption. In addition, an evaluation of the training program was planned as an instructor-led group discussion involving all employees.

Delivering the training. The third phase of the action research intervention was delivering the training. In terms of UCIT, this phase included delivering the learning task in the learning environment (see Figure 2).

Table 4. Determination of Instructional Task, Required Skills and Knowledge, Users' Current Level of Skills and Knowledge, and Corresponding Learning Tasks

Determination of Instructional Task	Knowledge and Skills Required	Problem with Users' Current level of Skills and Knowledge	Learning Tasks
To increase encryption of confidential e-mail	Knowledge of the existence and content of the e-mail policy, skills to apply information classification rules, skills to use e-mail encryption	Lack of skills to apply the information classification rules (i.e., to discover what information needs to be protected), lack of skills to use e-mail encryption	(1) To learn to apply the information classification rules (all users) (2) To learn to use e-mail encryption software (nontechnical users)

Before the training was delivered, the company's IS security manual was converted from an MS Word document to an HTML document (Table 3, content of the e-mail policy). In addition, to make the security manual easier to read, an abstract was added at the beginning of each section of the manual.

The first session was first held with the technical staff. The researcher and the IS security manager acted as the instructors. When the session started, all but two of the learners arrived late, and the atmosphere was hostile. For example, one software developer stated at the beginning of the session,

> *I have more important things to do than attend lectures on IS security. Such training is of no use to me or our team.*

Despite this, the session was delivered as planned during the second phase of the action research cycle. Surprisingly, the discussion concerning the threats to e-mail was lively. During the discussion, it became obvious that the technical users were willing to protect their company's valuable information, but they lacked the means to do this when using S/MIME encryption was not possible.

The use of the learners' own e-mail documents in the training was fruitful. The learners found that they had sent a lot of confidential information unencrypted, including technical details of the design of the products and pricing information. The employees also became more aware of the serious economic consequences for their team and the company if this confidential information would leak to their competitors. For example, they realized that losing product development information to the competitors would mean that a competitor could get the company's results and investments in years of work without any investment of their own. This could result in losing competitive advantage, which the company has tried to obtain with investment in product development, to a competitor. The learners agreed that such a situation must be avoided by encrypting e-mail messages. Consequently, to overcome the problems with S/MIME, the IS security manager proposed that the 7zip program should be tested for e-mail encryption. This was accepted by everyone. Finally, all technical users knew how to use 7zip. Hence, it was not necessary to practice.

Similar training sessions were also held with the company's six nontechnical users. They admitted that they do not comply with the e-mail policy. A lot of confidential information that should not be revealed to competitors was found in these users' unencrypted e-mails. Such confidential information included pricing information and confidential information on the design and technical characteristics of the company's own products. The users agreed that this situation needed to change. Since these six users did not know how to use 7zip, it was demonstrated in a second session. With the help of the researcher and the IS security manager, the users practiced using 7zip by sending and receiving 7zip-encrypted files.

In addition to these three training sessions, the researcher had three personal discussion sessions with the CEO regarding the employees' perception of the CEO's inactivity regarding IS security. In these discussions, the researcher encouraged the CEO to promote IS security and set an example by complying with the company's IS security policies and instructions.

Evaluating the results. The fourth phase of the action research intervention evaluated the results of the training, and included the fourth phase of UCIT. To this end, all of the users were interviewed at least twice: in a personal interview and a group interview. Informal social interactions, such as lunch breaks and training sessions at the gym, were also utilized for this purpose. In addition, participatory observation was used to collect information. Overall, the results of the first action research cycle were positive. The IS security manager was positive about the training program.

> *The users' attitude toward IS security issues is more positive than before the program. This was last seen at a project meeting with a customer: one of our software developers spontaneously suggested that 7zip-encryption with project-specific passwords*

> *should be brought in (instead of unencrypted e-mail messages). This practice was agreed [to] by all participants, and it is now the practice in that project. In addition, our sales assistant has spontaneously started to encrypt all board meeting agendas and notes before sending them. Hence, I consider the training program to have achieved its goal.*

In addition, nine users claimed that the training program made them think about the consequences of sending unencrypted e-mail. According to these users, this increased their use of e-mail encryption.

> *As a result of the training program, I have used e-mail encryption for the first time. My aim is to continue this practice.* (A sales team member)

> *I have seen an increase in the use of e-mail encryption among the sales team. I think that the biggest achievement of the training program has been making all of us more aware of the possible unwanted consequences of unencrypted e-mail. Hence, the training program achieved positive results. However, our team still tends to forget [to encrypt] e-mail.* (A sales team member)

Furthermore, 11 users argued that IS security procedures and the usability of the e-mail policy have been improved.

> *The new manual—including the e-mail policy—is quicker to access and the essential information is easier to find than in the old one.* (A technical expert)

Despite the positive results summarized in Table 5, four issues still needed to be addressed.

(1) The sales team in particular still took advantage of the permitted exceptions to e-mail encryption.

(2) The company's IS security manager felt that the training program would remain a one-off effort to increase users' IS security awareness. However, due to the positive results of the program, he believed that similar training should be given regularly in the future.

(3) Six users argued that the CEO was still considered too passive in promoting IS security issues. The users claimed this affected their motivation to comply with the company's IS security policies.

(4) The IS security manager and four other users felt that IS security issues were still too far removed from the company's other management and communication efforts. This was also claimed to have an impact on users' motivation to comply with IS security policies.

Of these four issues (Table 6), the first was addressed by continuing IS security training, while issues 2, 3, and 4 were tackled in the second research cycle by improving the company's prevailing IS security communication practices.

The Second Research Cycle at SC

While the first action research cycle focused on testing of the effectiveness of an intervention based on theory (UCIT and ELM), the second action research cycle sought to refine the intervention by incorporating a continuous IS security communication process. The first action research cycle was fully informed by theories (UCIT, ELM), but the second cycle tackled issues prompted by practice (issues 2, 3, and 4 in Table 6). The second cycle had the following three phases: (1) developing a new IS security communication and training process, (2) implementing the new process, and (3) evaluating the results.

Developing a new IS security communication and training process. In the first phase of the second research cycle, a new IS security communication and training process was sketched to improve the three unsolved problems (issues 2, 3, and 4 in Table 6). Such a solution was seen as ideal for four reasons. First, IS security training and other communication regarding IS security issues would become more closely integrated with the company's existing communication process. The IS security manager expected this to narrow the perceived gap between IS security training and other communication efforts. In addition, this would allow regular IS security awareness training that would be closely integrated with the company's other communication efforts. Second, the process would be continuous. Third, the process was aimed at activating the CEO to do more to promote IS security issues. This was expected to demonstrate management's active involvement in IS security issues. Fourth, the process would make it easier for employees to make development proposals and report IS security problems.

The company had in place a communication process that covered all business issues. Once a month, the company held a half-day meeting. Attendance at these meetings was compulsory for all employees. At the meetings, the status of product development, customer installation projects, and sales projects was covered by the management. The researcher suggested that these meetings should also be used to integrate IS security communication and regular training with the existing communication process. As a consequence, the researcher and the IS security manager designed a new IS security communication and training process.

Table 5. Summary of the Results Achieved During the First Research Cycle at SC

Result	Method	Source of Evidence
Improved usability of the e-mail policy	Interviews	st2, st4, o2, sd1, sd2, sd3, sd4, sd5, ts1, ts2, ts3
New encryption solutions to overcome technical problems	Interview	IS security manager
Improved consciousness of the possible consequences of not encrypting e-mail, resulting in increased use of encryption	Interviews	st2, st4, o2, sd1, sd2, sd3, ts1, ts2, ts3
Observed increase in the use of e-mail encryption	Participatory observation	Researcher
Increase in the use of e-mail encryption	Interviews	IS security manager, o1

Table 6. Issues Requiring Further Improvement After the First Research Cycle

Issues Still Requiring Improvement	Source	Planned Solutions
(1) Sales team e-mail encryption	st1, st2	Continuing training as described in the first research cycle
(2) The need for continuous training and discussions	IS security manager, st2	New IS security communication process to be developed during the second research cycle
(3) Perceived passiveness of management in setting an example	sd1, sd2, sd3, ts1, ts2, o2	New IS security communication process to be developed during the second research cycle
(4) IS security was at too great a distance from the company's daily business	sd1, sd3, ts1, ts2, IS security manager	New IS security communication process to be developed during the second research cycle

Table 7. Summary of the Results Achieved During the Second Research Cycle at SC

Result	Method	Source of Evidence
Dedicated IS security training sessions are not needed anymore. This has resulted in a better integration of IS security communication with other communication efforts.	Interviews	IS security manager, CEO
Continuous IS security awareness and discussion through monthly meetings.	Interviews	CEO, IS security manager, ts3
Increased activity on the part of the CEO.	Interviews	sd1, sd2, ts1, ts3, IS security manager
Observed increased activity on the part of the CEO	Participatory observation	Researcher
Increased activity on the part of the users.	Interviews	IS security manager, sd1
Observed increased activity on the part of the users	Participatory observation	Researcher

The company's IS security manager was nominated to be responsible for gathering development proposals and problem reports from employees. Furthermore, it was his responsibility to make sure that all reported problems were solved in a timely fashion. In addition, he was responsible for allocating resources to IS security development tasks and coordinating their completion. His additional responsibilities included reporting solved and unsolved problems, as well as the progress of the development tasks, to the CEO. The CEO had overall responsibility for the process. He became respon-

sible for following up the problem reports and development tasks on a monthly basis and communicating their progress to employees at each monthly meeting.

Implementing the new process. The second phase of the second research cycle involved implementing the new IS security communication process. During implementation of the new process, the company's IS security manager left the company. The legal advisor then became the new IS security manager and consequently was responsible for implementing the new communication process. However, his unfamiliarity with the company's security posture became another barrier to implementing the new IS security communication process. As the legal advisor (new IS security manager) explains,

> *At first, I did not feel comfortable being responsible for the company's IS security issues. I did not get any introduction to security issues. Also, my workload was high even without these new responsibilities.*

Due to the new IS security manager's inexperience, one of the researchers had to help him to cope with his everyday IS security work and the implementation of the new process. Moreover, as the CEO still remained passive, the researcher continued to try to persuade the CEO to take a more active role in IS security matters. After three months, the CEO realized the severity of the prevailing situation, and he started promoting IS security issues. The new IS security manager also became more familiar with his responsibilities, and was able to restart the IS security development efforts. Finally, after five months, as both key persons were able to take responsibility for the company's IS security management and development, the new communication process started to work as described below.

Evaluating the results. The third phase of the second research cycle involved evaluating the results achieved. The new IS security communication process is currently in operation, with the result that there has been no need for dedicated IS security policy compliance training sessions, as the monthly meetings have been regularly used for IS security policy compliance training.

At the beginning of the implementation of the new communication process, the employees perceived the CEO as being completely inactive in presenting IS security issues to the staff. However, this changed. Afterward, he regularly participated in communicating IS security issues. Consequently, the users seemed to perceive management as being more active in IS security issues. In fact, five users reported that this had improved their motivation to comply with IS security policies. The CEO's increased activity had also been observed by the researcher. Furthermore, the new IS security manager had noticed that users were actively participating in IS security discussions. According to the IS security manager, this also resulted in several spontaneous IS security development efforts by the users. These positive results of the second research cycle at SC are summarized in Table 7.

Discussion

This paper discusses the development of an IS security policy compliance training program. The development of the training program was based on two theories: UCIT and ELM. This program was tested and refined at a software company through an action research intervention. The first column in Table 8 summarizes the key findings based on this empirical intervention. The second column points out whether the finding supports the two reference theories (UCIT and ELM), or if the findings emerged from the action research intervention. The third column illustrates examples of the related findings in other fields. Findings 1 through 4 (Table 8) stemmed from the first action research cycle aimed at testing the IS security policy compliance training program. The first action research cycle was informed by the theories of UCIT and ELM, and was oriented toward theory-testing. The findings from the first action research cycle supported these theories. To maximize employees' compliance with the IS security policies, our action research intervention suggested that an IS security communication process was needed, in addition to an IS security training program. The second action research cycle focused on theory refinement by extending the IS security training program with an IS security communication process. Findings 5 through 9 (Table 8) originated from the second action research cycle; hence they stem from the action research intervention rather than a theory.

Of the nine key findings (Table 8), we would like to highlight especially that information security training should utilize methods and learning tasks that activate and motivate the learners to perform systematic cognitive processing of information (findings 1 and 2). We also emphasize that information security training and communication efforts should be continuous and integrated into the organization's normal communication efforts (findings 5 and 6).

To the best of our knowledge, findings 1, 3, 8, and 9 are new in the area of IS security education (Table 8). In other words, we find no studies in the IS security training literature that have reported similar findings. With respect to the second finding, there appear to be no previous studies on IS security that have reported this. The closest is a study by Mitnick (2002), suggesting the use of media reports on security attacks

Table 8. Key Findings of the Study

Finding	Provided Empirical Support for or Stems From	Related Findings in Other Fields
1. IS security policy compliance training should use training methods that enable learners' systematic cognitive processing of information.	ELM	This result is consistent with the findings in other fields, such as in the area of the psychology of learning (Kolb 1984) and instructional design (Schott and Driscoll 1997).
2. IS security policy compliance training should use learning tasks that are of personal relevance to the learners.	ELM	This finding is also in synch with results in other fields. For example, Petty and Cacioppo (1981a, 1986) found that the personal relevance of the topic has a strong impact on learners' motivation. In addition, studies by Gardner (2004) and Clark (2003) found that learning tasks that are of personal relevance to the learners enhance learning, as suggested by ELM.
3. Successful IS security policy compliance training should take into account the learner's previous knowledge regarding IS security policy compliance.	UCIT	Similar findings have been reported in the area of instructional design (Schott and Driscoll 1997) and the psychology of learning (Bruner 1986; Vygotsky 1986).
4. Changing IS security behavior is difficult to achieve and requires adaptation of educational methods.	UCIT	Similar findings have been reported in the area of instructional design (Schott and Driscoll 1997).
5. In order to improve users' motivation to comply with the IS security policies, integrate IS security training with normal business communication of the organization.	Stemmed from the action research intervention	This result is consistent with the findings in the area of social psychology arguing that the context and situational conditions of the communication influence the receiver's motivation (Bohner and Wänke 2002).
6. There should be a process to make IS security communication a continuous activity rather than one-off efforts to increase employees' IS security policy compliance.	Stemmed from the action research intervention	The present study supports the earlier findings in the area of communication presenting that communication should be a continuous process to achieve collective action between the communicating parties (Figueroa et al. 2002; Rogers and Kincaid 1981).
7. Top management support is important for ensuring employees' compliance with the security policies.	Stemmed from the action research intervention	The importance of top management's support to organizational change has been reported in strategic IS planning (Kearns 2006).
8. The activation of users through active discussion and education results in IS security problem reports and IS security development efforts.	Stemmed from the action research intervention	This result is consistent with the findings in the areas of the psychology of learning (Kolb 1984) and instructional design (Schott and Driscoll 1997).
9. Involving management, IS security staff, and users in a continuous, active IS security flow of communication to achieve improved IS security policy compliance through consensus.	Stemmed from the action research intervention	The present study supports the earlier findings in the area of communication, that information should be actively shared among teh communicating parties to achieve consensus between the parties (Figueroa et al. 2002; Rogers and Kincaid 1981).

and how these attacks could be avoided. However, the underlying learning principles of this strategy were not discussed, with the result that educators do not have the information about how and why this strategy is expected to work.

As for the fourth finding, we conclude that changing IS security behavior is difficult to achieve and requires adaptation of educational methods. To our knowledge, all the extant studies on IS security training (N = 23, Table 1) emphasize training as a potential means to achieve behavioral change. However, these IS security studies do not discuss the adaptation of cognitive educational methods, nor do they mention the empirical findings of such adaptation for achieving behavioral change through planned cognitive training.

The fifth implication for practice, integrating IS security training with other communication, ensures that employees do not perceive IS security as a separate issue that has little connection to the normal work of the employees and business activities of the company. When IS security communication is integrated with normal business communications, employees see that the IS security issues relate to their normal work. Such integration also implies to the employees that IS security is part and parcel of the organization's business function and it belongs to each employee's work task. Our findings suggests that this, in turn, has an impact on users' motivation to comply with IS security policies. While IS security training studies suggest the distribution of messages on the importance of IS security compliance through e-mail,

posters, and coffee mugs (Murray1991; Peltier 2002; Rudolph et al. 2002), these studies do not discuss the integration of IS security communication into normal business communication channels.

With respect to the sixth finding, previous IS security studies (Gaunt 1998; McLean 1992) have postulated that there should be a process to make IS security communication a continuous activity rather than one-off efforts to increase employees' IS security awareness and policy compliance. However, these existing IS security studies do not offer any empirical evidence to support this claim. This study is the first to provide empirical evidence of the importance of making IS security communication a continuous activity instead of a one-off effort.

The same goes for finding 7 (Table 8). In the present study, we found evidence that supports the previous anecdotal view that top management support is important for ensuring employees' compliance with the security policies. While previous IS security studies mentioned the importance of visible top management support (Murray 1991; Perry 1985; Wood 1995), we found no empirical studies that have confirmed this.

Implications for Practice

We would like to highlight seven implications for IS security educators in organizations (Table 9). The first implication for practice stresses the need for the use of a systematic IS security training program. Such training programs are useful for skill training and improving attitudes toward IS security policy compliance. Training programs are also a good means of paving the way to continuous IS security communication. This means that practitioners should note that in order to increase employees' IS security awareness and policy compliance, one-off training efforts alone are not enough. In addition, there should be a process for making IS security communication a continuous activity in the organization.

The second implication for practice, providing IS security training, calls for the use of learning tasks that are of personal relevance to the learners, so there are visible consequences for the self and others. An example of this in the context of sending confidential information through e-mail without encryption is to extract sensitive information from actual e-mail documents and discuss with the employees the negative consequences of sending those documents unencrypted.

The third practical implication, using IS security policy compliance training methods and ideas, enables employees' long-lasting learning through cause-and-effect mental models. This can be achieved by making employees explore the possible unwanted consequences of their own actions. An example of an unwanted consequence is a leakage of confidential information to a competitor by sending it unencrypted via e-mail. This could lead to losing competitive advantage to the competitor.

To achieve the fourth implication for practice, designing IS security policy compliance training, surveys and interviews are useful. Surveys are useful for collecting anonymous information, while interviews help to get an in-depth understanding of the users' perceptions. In the actual training, employees should be divided into different training groups according to their knowledge, to ensure that learners' previous knowledge is taken into account.

In order to meet the fifth implication for practice, integrating IS security training, the existing normal communication channels can be used for regular IS security communication, as happened at SC. Other potential communication channels include the management's business reviews, existing training programs and staff magazines and bulletins.

To achieve the sixth implication, ensuring that users comply with IS security policies, our results suggest that ensuring top management's visible support for IS security requires regular promotion of IS security issues through existing communication channels, such as management reviews, the intranet and personnel magazines. In addition to active promotion, top management's support becomes visible in the managers' exemplary behavior in terms of IS security policy compliance.

In order to meet the seventh implication for practice, improving IS security, users should be encouraged to report IS security issues and participate in IS security development efforts by different means. In our case, the users were activated by training sessions and the new continuous IS security communication process and a security tracking system that allowed them to monitor the progress of all IS security development efforts.

Limitations and Implications for Future Research

This study took place in a relatively small organization in Finland where all employees hold a university or college degree. Therefore, future research is needed to study the challenges in increasing employees' compliance with IS security policies in organizations of different sizes and in different countries/cultures. Furthermore, SC operated in a highly turbulent business environment. Organizations operating in a more stable business environment may experience other challenges, as

Table 9. Implications for Practice	
1.	Use a systematic training program when designing and implementing IS security training programs.
2.	When providing IS security training, use learning tasks that are of personal relevance to the learners, so there are visible consequences for the self and others.
3.	Use IS security policy compliance training methods and ideas that enable learners' systematic cognitive processing of information.
4.	When designing IS security policy compliance training, practitioners should take into account the learners' previous knowledge regarding IS security policy compliance.
5.	Integrate IS security training with normal business communication efforts in order to eliminate employees' perceptions of IS security as a separate issue from business function and employees' work tasks.
6.	To ensure that users comply with IS security policies, visible support of IS security by top management is necessary.
7.	Improve IS security by activating employees to discuss security through educational sessions.

they are not used to changing their operations at a fast pace. Hence, future research is needed to explore the usefulness of our findings in organizations that operate in a stable environment, have employees of various ages and levels of education, have different organizational cultures, and have IS security policies of varying complexity. As our study focused on e-mail encryption, future research should study how these principles work in other contexts, such as non-work related use of the Internet and IS at work. Furthermore, this study focused on an issue requiring users' motivation to comply with policies, rather than the learning of complicated technical knowledge or skills. This was achieved by utilizing training methods that enable users' cognitive processing of information received during the training. Since we did not study whether a similar approach is also appropriate for more technically oriented subjects (e.g., development of a secure IS or firewall configuration) and target groups (e.g., IS developers or IS administrators), future research should study this issue.

Another research topic is the role of management visibility in employees' compliance. Wylder (2003) challenged the significance of visible management support with respect to IS security policy compliance by arguing that top management commitment to security policy has no bearing on ordinary employees' attitudes and commitment toward security policy. Wylder argues that managers are too far removed from the day-to-day activities of organizations. Our study contradicts Wylder's view, and we call upon future researchers to further investigate this issue. Since our results were obtained in a small organization, future studies are needed to study this issue, especially in large organizations.

Furthermore, in addition to training and continuous communication, the role of campaigns in improving employees' IS security policy compliance should be studied. Since campaigns have proved successful in changing human behavior in different contexts, such as highway safety (Rodriguez and Anderson-Wilk 2002), their potential in the IS security field should be studied. While the use of campaigns has been noted in IS security literature (McLean 1992; Proctor and Byrnes 2002; Rudolph et al. 2002; Wood 2002), we found no empirical studies reporting practical experiences of IS security campaigns. Moreover, while in-house change agents have been successfully used in other fields to promote organizational change (Cockman et al. 1999; Paton and McCalman 2004), we have seen no studies on change agents with respect to IS security policy compliance. In the context of IS security policy compliance, the change agents would not only show a positive example in complying with IS security policies, but also encourage and persuade people to comply with the policies. Future research should examine the use of change agents in gaining employees' compliance with IS security policies.

Finally, in addition to training and other communication efforts, punishment (e.g., Mitnick 2002, Puhakainen 2006, Straub 1990) and rewards (e.g., Mitnick 2002, Puhakainen 2006) have also been suggested as possible means to increase compliance with IS security policies. The present study focused on training alone. Thus, future IS security policy compliance training studies should study whether the results of training programs can be enhanced by complementing training programs with rewards or sanctions.

Conclusions

Employees who do not comply with information security policies are a serious risk for their companies. To ensure compliance, different IS security policy compliance approaches have been advanced, ranging from sanctions and campaigns to training and education. Of these different compliance approaches, training and education are the most com-

monly suggested approaches in the literature. Despite this pattern in the literature, studies on IS security training and education approaches have largely remained atheoretical and anecdotal.

To address this deficiency in IS security policy compliance research, this paper developed a theory-based training program for IS security policy compliance training. The training program was based on the universal constructive instructional theory and the elaboration likelihood model. This paper then tested the practical workability of the training program through an action research intervention.

The training program proved to be useful in developing goal-oriented, effective IS security compliance training. One of our most important findings was that it is useful to use IS security policy compliance training methods and ideas that enable learners' systematic cognitive processing of information. Moreover, when providing IS security training, learning tasks that are of personal relevance to the learners should be used. In addition, IS security policy compliance training should take into account the learners' previous knowledge regarding IS security policy compliance. Another important finding was that integrating IS security communication with other communication efforts narrows the perceived gap between IS security training and other communication efforts. In fact, during the action research intervention, we realized that, in addition to training, continuous IS security policy compliance communication was needed to maximize employees' IS security policy compliance. The findings also indicate that visible support of IS security by top management is necessary to ensure that users comply with IS security policies.

These findings shed new light on how to tackle a key problem in organizations: employee lack of compliance with IS security policies. Finally, future research is needed to study the challenges in achieving a positive change in employees' compliance with IS security policies in organizations of different sizes. Future research should also investigate the use of change agents and IS security campaigns in gaining employees' compliance with IS security policies.

Acknowledgments

The authors wish to thank the senior editor, associate editor, and anonymous reviewers for their insightful comments and recommendations that contributed to significant improvements in the paper. They also wish to thank Gregory Moody, Anthony Vance, and Mari Karjalainen for their valuable feedback on early versions of the paper. Finally, they wish to thank the Finnish Funding Agency for Technology and Innovation for financial support.

References

Akers, R. L., and Sellers, C. S. 1994. *Criminological Theories: Introduction, Evaluation, and Application*, Los Angeles: Roxbury Publishing.

Arvey, R. D., and Ivancevich, J. M. 1980. "Punishment in Organizations: A Review, Propositions, and Research Suggestions," *The Academy of Management Review* (5:1), pp. 123-132.

Backhouse, J., and Dhillon, G. 2001. "Current Directions in IS Security Research: Toward Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp. 127-153.

Baskerville, R. 1999. "Investigating Information Systems with Action Research," *Communications of the Association for Information Systems* (2:19).

Baskerville, R., and Myers, M. 2004. "Special Issue on Action Research in Information Systems: Making IS Relevant to Practice-Foreword," *MIS Quarterly* (28:3), 329-335.

Baskerville, R., and Siponen, M. 2002. "An Information Security Meta-policy for Emergent Organizations" *Journal of Logistics Information Management, special issue on Information Security* (5-6), pp. 337-346.

Baskerville, R. and Wood-Harper, T. 1998. "Diversity in Information Systems Action Research Methods," *European Journal of Information Systems* (7:2), 1998, pp. 90–107.

Bohner, G., and Wänke, M. 2002. *Attitudes and Attitude Change*, Hove, England: Psychology Press.

Bruner, J. 1996. *Actual Minds, Possible Worlds*, Cambridge, MA: Harvard University Press.

Clark, R. 2003. *Building Expertise, Cognitive Methods for Training and Performance Development*, Washington DC: International Society for Performance Improvement.

Cockman, P., Evans, B., and Raynolds, P. 1999. *Consulting for Real People: A Client-Centered Approach for Change Agents and Leaders*, Maidenhead, England: McGraw-Hill.

Cox, A., Connolly, S., and Currall, J. 2001. "Raising IS Security Awareness in the Academic Setting," *VINE* (31:2), pp. 11-16.

CSI/FBI. 2007. "CSI Survey 2007: The 12th Annual Computer Crime and Security Survey," Computer Security Institute (available online at http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf).

Desman, M. B. 2002. *Building an IS Security Awareness Program*, Boca Raton, FL: Auerbach Publications.

Dhillon, G. 1997. *Managing Information System Security*, London: Macmillan, 1997.

Dick, W., and Carey, L. 1996. *The Systematic Design of Instruction*, New York: Harper Collins.

Feyerabend, P. K. 1964. "Realism and Instrumentalism," in *The Critical Approach to Science and Philosophy*, M. Bunge (ed.), London: Free Press of Glencoe, pp. 280-308.

Figueroa, M. E., Kincaid, D. L., Rani, M., and Lewis, G. 2002. *Communication for Social Change: An Integrated Model for Measuring the Process and Its Outcomes*, New York: Rockefeller Foundation.

Gagné, R. M. 1985. *The Conditions of Learning*, New York: CBS College Publishing.

Galliers, R. D. 1992. "Choosing Information Systems Research Approaches," in *Information Systems Research: Issues, Methods, and Practical Guidelines*, R. D. Galliers (ed.), Oxford, England: Blackwell Scientific Publications, pp. 144-162.

Gardner, H. 2004. *Changing Minds: The Art and Science of Changing Our Own and Other People's Mind*, Boston: Harvard Business School Press.

Gaunt, N. 1998. "Installing an Appropriate IS Security Policy [in Hospitals]," *International Journal of Medical Informatics* (49:1), pp. 131-134.

Glaser, R. 1971. "The Design of Instruction," in *Instructional Design: Readings*, M. D. Merrill (ed.), Englewood Cliffs, NJ: Prentice-Hall.

Goodhue, D. L., and Straub, D. W. 1991. "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security," *Information & Management* (20), pp.13- 27.

Greenwald, A. G. 1968. "Cognitive Learning, Cognitive Response to Persuasion, and Attitude Change," in *Psychological Foundations of Attitudes*, A. G. Greenwald, T. C. Brock, and T. M. Ostrom (eds.), San Diego, CA: Academic Press, pp. 147-170.

Guba, E. G., and Lincoln, Y. S. 1989. *Fourth Generation Evaluation*, Newbury Park, CA: Sage Publications.

Hadland, T. 1998. "IS Security Management: An Awareness Campaign," in *UKOLUG98: New Networks, Old Information—UKOLUG's 20th Birthday Conference*, C. J. Armstrong and R. J. Hartley (eds.), Manchester, England, July 14-16.

Hung, D. 2001. "Theories of Learning and Computer-Mediated Instructional Technologies," *Educational Media International* (38:4), pp. 281-287.

Kajava, J., and Siponen, M. T. 1997. "Effectively Implemented IS Security Awareness: An Example from University Environment," in *Information Security in Research and Business (Proceedings of IFIP TC 11 13th International Conference on IS Security)*, L. Yngström and J. Carlsen (eds.), London: Chapman and Hall.

Karjalainen, M. 2009. *Review of IS Security Training Approaches: Implications for Practice and Research*, unpublished Licentiate thesis, University of Oulu, Finland.

Kearns, G. 2006. "The Effect of Top Management Support of SISP on Strategic IS Management: Insights from the US Electric Power Industry," *Omega* (34:3), pp. 236-253.

Kolb, D. A. 1984. *Experiential Learning: Experience as the Source of Learning and Development*, Englewood Cliffs, NJ: Prentice-Hall, 1984.

Lafleur, L. M. 1992. "Training as Part of a Security Awareness Program," *Computer Control Quarterly* (10:4), pp. 4-11.

Lakatos, I. 1970. "Falsification and the Methodology of Scientific Research Programmes," in *Criticism and the Growth of Knowledge*, I. Lakatos and A. Musgrave (eds), Cambridge, UK: Cambridge University Press, pp. 91-196.

Laudan, L. 1984. *Science and Values*, Berkeley, CA: University of California Press.

McGuire, W. J. 1968. "Personality and Attitude Change: An Information-Processing Theory," in A. G. Greenwald, T. C. Brock, and M. T. Ostrom (eds.), *Psychological Foundations of Attitudes*, San Diego: Academic Press, pp. 171-196.

McLean, K. 1992. "IS Security Awareness— Selling the Cause," in *Information Technology Security: The Need for International Cooperation (Proceedings of the IFIP TC11, Eighth International Conference on Information Security)*, G. G. Gable and W. J. Caelli (eds.), May 27-29, Amsterdam: North-Holland Publishing Co., pp. 179-193.

Myers, M., and Newman, M. 2007. "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization* (171), pp. 2-26.

Mitnick, K. D. 2002. *The Art of Deception: Controlling the Human Element of Security*, New York: Wiley Publishing.

Murray, B. 1991. "Running Corporate and National Security Awareness Programs," in *Proceedings of the IFIP TC11 Seventh International Conference on IS Security*, Amsterdam: North-Holland Publishing Co., pp. 203-207.

Mårtensson, P., and Lee, A. S. 2004. "Dialogical Action Research at Omega Corporation," *MIS Quarterly* (28:3), pp. 507-536.

NIST. "An Introductio to Computer Security: The NIST Handbook," Special Publication 800-12, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce (available at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

NIST. "Information echnology Security Training Requirements: A Role- and Performance-Based Model," NIST Special Publication 800-16, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology (available at http://csrc.nist.gov/publications/nistpubs/800-16/ 800-16.pdf).

Paton, R. A., and McCalman, J. 2004. *Change Management: A Guide to Effective Implementation* (2nd ed.), Newbury Park, CA: SAGE Publications.

Peltier, T. 2002. "How to Build a Comprehensive Security Awareness Program," *Computer Security Journal* (16:2), pp. 23-32.

Peltier, T. 2002. *IS security Policies, Procedures, and Standards: Guidelines for Effective IS security Management*, Boca Raton, FL: Auerbach Publications.

Perry, W. E. 1985. *Management Strategies for Computer Security*, Newton, MA: Butterworth-Heinemann.

Petty, R. E., and Cacioppo, J. T. 1981a. *Attitudes and Persuasion: Classic and Contemporary Approaches*, Dubuque, IA: Brown.

Petty, R. E., and Cacioppo, J. T. 1981b. "Issue Involvement as a Moderator of the Effects on Attitude of Advertising Content and Context," *Advances in Consumer Research* (8), pp. 20-24.

Petty, R. E., and Cacioppo, J. T. 1984. "Source Factors and the Elaboration Likelihood Model of Persuasion," *Advances in Consumer Research* (11), pp. 668-672.

Petty, R. E., and Cacioppo, J. T. 1986. "The Elaboration Likelihood Model of Persuasion," in *Advances in Experimental Social Psychology* (19), L. Berkowitz (ed.), San Diego: Academic Press, pp. 123-205.

Popper, K. R. 1968. *The Logic of Scientific Discovery*, London: Hutchinson.

Proctor, P. E., and Byrnes, F. C. 2002. *The Secured Enterprise: Protecting Your Information Assets*, Upper Saddle River, NJ: Prentice Hall.

Puhakainen, P. 2006. *A Design Theory for Information Security Awareness*, unpublished Ph.D. Thesis, University of Oulu, Finland.

Rest, J. R. 1994. "Background: Theory and Research," in *Moral Development in the Professions: Psychology and Applied Ethics*, J. R. Rest and D. Narvaéz (eds.), Hillsdale, JJ: Lawrence Erlbaum Associates, pp. 1-26.

Rodriguez, L., and Anderson-Wilk, M. 2002. "Communicating Highway Safety: What Works," CTRE Project 01-85, Iowa Safety Management System, Center for Transportation Research and Education, Iowa State University, Ames, Iowa (available at http://ntl.bts.gov/lib/22000/22800/22892/chs.pdf).

Rogers, E. M., and Kincaid, D. L. 1981. *Communication Networks: Toward a New Paradigm for Research*, New York: Free Press.

Rudolph, K., Warshawsky, G., and Numkin, L. 2002. "Security Awareness," in *Computer Security Handbook* (4th ed.), S. Bosworth and M. E. Kabay (eds.), New York: John Wiley & Sons, pp. 29.1-29.19.

Schott, F., and Driscoll, M. P. 1997. "On the Architectonics of Instructional Theory," in *Instructional Design: International Perspective, Vol. 1, Theory, Research, and Models*, R. D. Tennyson, F. Schott, N. Seel, and S. Dijkstra (eds.),Mahwah, NJ: Lawrence Erlbaum Associates, pp. 135-173.

Senge, P. M, Kleiner, A. C., Ross, R., and Smith, B. 1994. *The Fifth Discipline Fieldbook*, New York: Doubleday.

Siponen, M. 2000a. "A Conceptual Foundation for Organizational IS Security Awareness," *Information Management & Computer Security* (8:1), pp. 31-41.

Siponen, M. 2000b. "On the Role of Human Morality in Information System Security: The Problems of Descriptivism and Non-Descriptive Foundations," in *Information Security for Global Information Infrastructures (Proceedings of the IFIP TC11 Fifteenth Annual Working Conference on IS Security*, S. Qing and J. H. P. Eloff (eds.), Boston: Kluwer Academic Publishers, pp. 401-410.

Siponen, M. T., Pahnila, S., and Mahmood, A. 2007. "Employees' Adherence to Information Security Policies: An Empirical Study," in *New Approaches for Security, Privacy and Trust in Complex Environments (Proceedings of the 22nd IFIP TC 11 International Information Security Conference*), H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms (eds.), Boston: Springer, pp. 133-144.

Spurling, P. 1995. "Promoting Security Awareness and Commitment," *Information Management and Computer Security* (3:2), pp. 20-26.

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441-469.

Telders, E. 1991. "Security Awareness Programs: A Proactive Approach," *Computer Security Journal* (7:2), pp. 57-64.

Thomson, M. E., and von Solms R. 1997. "An Effective IS Security Awareness Program for Industry," in *Information Security in Research and Business (Proceedings of IFIP TC 11 13th International Conference on IS Security)*, L. Yngström and J. Carlsen (eds.), London: Chapman and Hall.

Thomson, M. E. and von Solms, R. "IS Security Awareness: Educating Your Users Effectively," *Information Management & Computer Security* (6:4), 1998, pp. 167-173.

Tudor, J. K. 2001. *IS Security Architecture: An Integrated Approach to Security in the Organization*, Boca Raton, FL: Auerbach Publications.

von Solms, R. 1999. "Information Security Management: Why Standards Are Important," *Information Management and Computer Security* (7:1), pp. 50-58.

Vroom, C., and von Solms, R. 2002. "A Practical Approach to IS Security Awareness in the Organization," in *Security in the Information Society: Visions and Perxpectives (Proceedings of IFIP TC 11 17th International Conference on IS Security)*, A. Ghonaimy, M. T. El-Hadidi, and H. K. Aslan (eds.), Boston: Kluwer Academic Press, pp. 19-38.

Vygotsky, L. 1986. *Thought and Language*, Cambridge, MA: MIT Press.

Walsham, G. 2o06. "Doing Interpretive Research," *European Journal of Information Systems* (15:3), pp. 320-330.

Wood, C. C. 1995. "Information Security Awareness Raising Methods," *Computer Fraud & Security Bulletin*, June, pp. 13-15.

Wood, C. C. 2002. "The Human Firewall Manifesto," *Computer Security Journal* (18:1), pp. 15-18.

Wylder, J. O. 2003. "Improving Security From the Ground Up," *Information Systems Security* (11:6), pp. 29-38.

About the Authors

Petri Puhakainen is a senior researcher in the Security Research Centre, Department of Information Processing Science at the University of Oulu, Finland. He holds a Ph.D. in Information Processing Science from the University of Oulu, Finland, and the degrees of L.Sc. (Tech.) and M.Sc. (Tech.) in Computer Science from the Helsinki University of Technology. His research interests include IS security behavior, IS security awareness and training, and IS security maturity. Dr. Puhakainen has been involved in the field of information systems and IS security for over 20 years as a security director, consultant, teacher, and researcher.

Mikko Siponen is a professor and director of the IS Security Research Centre in the Department of Information Processing Science at the University of Oulu, Finland. He holds a Ph.D. in Philosophy from the University of Joensuu, Finland, and a Ph.D. in Information Systems from the University of Oulu. His research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. He has 30 published or forthcoming papers in journals such as *Journal of the Association for Information Systems, European Journal of Information Systems, Information & Organization, Information Systems Journal, Information & Management, DATA BASE, Communications of the ACM, IEEE Computer,* and *IEEE IT Professional*. He has served as a senior and associate editor for the International Conference on Information Systems aswell as guest senior editor for the *MIS Quarterly* special issue on Information Systems Security in a Digital Economy. He is a member of the editorial boards of *European Journal of Information Systems, Journal of Organizational and End User Computing,* and *Journal of Information Systems Security.*

MIS Quarterly

RESEARCH ARTICLE

IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY

By: **Petri Puhakainen**
IS Security Research Center
Department of Information Processing Science
University of Oulu
Oulu
FINLAND
petri.puhakainen@oulu.fi

Mikko Siponen
IS Security Research Center
Department of Information Processing Science
University of Oulu
Oulu
FINLAND
mikko.siponen@oulu.fi

Appendix A

A Questionnaire for Planning IS Security Awareness Training at SC

1. In your opinion, what are the most common ways malicious software (viruses etc.) gets into our company's network?
2. Where can you find our company's official information security instructions?
3. Have you applied the instructions concerning SC's e-mail use to your work? If yes, give some examples of what instructions and for what purposes they were used.
4. Did you find the instructions useful for your purposes? Were they easy to understand and use in practice? Why or why not?
5. Explain briefly the purpose of our company's information classification rules.
6. How have you applied the information classification rules in your work (i.e., in practice)?
7. How much time do you spend processing e-mail (company's e-mail account) on a weekly basis? (Your best estimate)
8. For what purposes do you use e-mail in your work?
9. What do you consider as acceptable use of our company's e-mail system?
10. Give examples of what you consider unacceptable use of our company's e-mail system?
11. Have you ever encountered malicious software in e-mail attachments? Did this happen at SC or somewhere else? Explain what happened.
12. Have you ever followed (clicked and opened a page) a specially crafted, malicious link in an e-mail message? Did this happen at SC or somewhere else? What happened?
13. How many spam messages do you receive at our company's e-mail account (e.g., on a weekly basis)? Also give an estimate of how many received messages (e.g., percentage) are spam. Have you ever tried to answer any of the spam messages?
14. In your opinion, by what means is it possible to distinguish relevant e-mail messages from spam or other possibly dangerous messages?
15. By what means would you ensure it is safe to open an e-mail attachment?

16. In your opinion, for what general reasons should digital signing be used when sending e-mail messages via the Internet?
17. In your opinion, what kind of information should be digitally signed in your own work-related e-mail messages?
18. In your opinion, what kind of content should be encrypted in your own work-related e-mail messages?
19. Do you consider using e-mail encryption and digital signatures to be difficult? Why?
20. Have you ever encrypted work-related e-mail messages? For what reasons did you encrypt them?
21. If the receiver (e.g., a customer company) does not have a compatible e-mail encryption/decryption system, are you able to encrypt information in some other way? How would you do this?
22. Are there any other security issues that you consider important for your work?

Appendix B

Methodological Details

Principles for Conducting the Research Interviews

Stinger (1999) argues that a major problem with interviews is that the researcher's perceptions, perspectives, interests, and agendas easily influence questions (see also Myers and Newman, 2007). To avoid this, we used an approach proposed by Spradley (1979). This approach suggests that the researcher ask questions that are relatively neutral. This is necessary to diminish the extent to which participants' perceptions will be governed by frameworks of meaning unintentionally imposed by the researcher. Spradley advises the researcher to start with general questions that are sufficiently global to enable participants to describe their situation in their own terms. When the researcher wants to gain more detailed information, he can present a set of questions that focus on concepts already presented. In all phases of the interview, the researcher should take a neutral stance and write down or record the responses as accurately as possible. In this action research study, the researchers followed Spradley's approach in all interviews.

Principles for Evaluating the Validity of the Action Research Intervention

According to action research, theories are validated through their successful use (Baskerville and Myers 2004; Stinger 1999). Baskerville and Wood-Harper (1998) proposed seven validity criteria for IS action research: (1) the research should be set in multivariate social situations; (2) the observations should be recorded and analyzed in an interpretive frame; (3) researcher actions should intervene in the research setting; (4) the method of data collection should include participatory observation; (5) changes in the social setting should be studied; (6) the immediate problem in the social setting must have been resolved during the research; and (7) the research should illuminate a theoretical framework that explains how the actions led to a favorable outcome. More recently, Baskerville and Myers (2004) laid down four critical elements of action research: (1) there must be an explicit underlying theory before an action; (2) there must be practical action; (3) the theory should be adjusted according to the practical outcome; and (4) the action must be socially situated. The criteria of Baskerville and Wood-Harper and the critical elements of Baskerville and Myers were applied in evaluating the action research study (see Table C1 in Appendix C).

Appendix C

Evaluating the Interventions from the Viewpoint of Action Research Validity Criteria

Table C1. Action Research Validity Criteria

The Action Research Validity Criteria (Baskerville and Wood-Harper 1998)	Explanation on how our study met each criteria
1. The research should be set in multivariate social situations	The action research intervention was set in a multivariate social situation. It was conducted with all the employees of the company, involving various relationships between the participants. In addition, the research involved complex business relationships between the company and its customers and partners.
2. The observations should be recorded and analyzed in an interpretive frame	The observations were stored and analyzed within an interpretive frame and a theory-based framework was developed to support the analysis of the research data. Each employee was interviewed at least twice: once during the problem analysis phase and once when the results of the first research cycle were evaluated. The interviews were stored throughout in the form of field notes. In addition to what was said, the body language of the interviewees was also observed and recorded. The aim was to increase the reliability of subsequent analysis by identifying issues for further clarification if the researcher believed that not all relevant issues had been made explicit. The first author of this paper stored all his observations, impressions and perceptions in a research diary for subsequent analysis.
3. Researcher actions should intervene in the research setting	The first author of this paper worked actively and directly with the employees of the host organization. He had the main responsibility for designing and delivering the IS security training program and the new IS security communication process. This also complies with the requirement of practical action (Baskerville and Myers 2004).
4. The method of data collection should include participatory observation	Interviews, participatory observation, and surveys were used. The first author of this paper had the opportunity to spend several months at the company. This provided a good opportunity for participatory observation, especially during the second research cycle. The IS security manager was also a valuable source of information.
5. Changes in the social setting should be studied	The outcome of the research project was assessed with reference to the practitioner-collaborators' views of the success of both the training program and the communication process. Not only the IS security manager, but also several other employees reported that the training program and the new process achieved its goal. This also fulfills the requirement of socially situated action (Baskerville and Myers 2004).

Table C1. Action Research Validity Criteria	
The Action Research Validity Criteria (Baskerville and Wood-Harper 1998)	**Explanation on how our study met each criteria**
6. The immediate problem in the social setting must have been resolved during the research	The immediate problem was resolved during the study, according to the evaluations made by the practitioner-collaborators. The practitioner-collaborators believed that their understanding of the risks relating to insecure use of e-mail increased and their compliance with the e-mail policy improved. In addition, according to the practitioner-collaborators' evaluations, the new communication process developed during the second action research cycle achieved its goal by integrating IS security communication with other communication efforts and by activating the CEO and users to discuss IS security policy compliance issues regularly. The second action research cycle fulfills the requirement for adjusting the theory to the practical outcome (Baskerville and Myers 2004) as the original theoretical framework for training was extended to cover continuous training and communication between users and management.
7. The research should illuminate a theoretical framework that explains how the actions led to a favorable outcome.	The actions within the first action research cycle were linked to the theoretical framework of the IS security policy compliance training program. This framework defined the requirements for the training and explained how the training led to a favorable outcome. This also complies with the requirement of an explicit underlying theory before an action (Baskerville and Myers 2004). The second research cycle aimed at further improving organizational issues that were perceived as a hindrance to IS security policy compliance. The actions within the second research cycle were also derived from a theoretical framework.

References

Baskerville, R., and Myers, M. 2004. "Special Issue on Action Research in Information Systems: Making IS Relevant to Practice-Foreword," *MIS Quarterly* (28:3), 329-335.

Baskerville, R. and Wood-Harper, T. 1998. "Diversity in Information Systems Action Research Methods," *European Journal of Information Systems* (7:2), 1998, pp. 90–107.

Myers, M., and Newman, M. 2007. "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization* (171), pp. 2-26.

Spradley, J. P. 1979. *The Ethnographic Interview*, Belmont, CA: Wadsworth.

Stinger, E. T. 1999. *Action Research* (2nd ed.), Thousand Oaks, CA: Sage Publications.