OULU 2006
A 463

ACTA UNIVERSITATIS OULUENSIS

Petri Puhakainen

A DESIGN THEORY FOR INFORMATION SECURITY AWARENESS

FACULTY OF SCIENCE,
DEPARTMENT OF INFORMATION PROCESSING SCIENCE,
UNIVERSITY OF OULU

ACTA UNIVERSITATIS OULUENSIS
A Scientiae Rerum Naturalium 463

PETRI PUHAKAINEN

A DESIGN THEORY FOR INFORMATION SECURITY AWARENESS

Academic Dissertation to be presented with the assent of the Faculty of Science, University of Oulu, for public discussion in Raahensali (Auditorium L10), Linnanmaa, on July 24th, 2006, at 12 noon

OULUN YLIOPISTO, OULU 2006

Acta Univ. Oul. A 463, 2006

Supervised by
Professor Mikko Siponen

Reviewed by
Professor Gurpreet Dhillon
Professor Reima Suomi

ISBN 951-42-8113-6 (Paperback)
ISBN 951-42-8114-4 (PDF) http://herkules.oulu.fi/isbn9514281144/
ISSN 0355-3191 (Printed)
ISSN 1796-220X (Online) http://herkules.oulu.fi/issn03553191/

Cover design
Raimo Ahonen

OULU UNIVERSITY PRESS
OULU 2006

Puhakainen, Petri, A design theory for information security awareness
Faculty of Science, Department of Information Processing Science, University of Oulu, P.O.Box 3000, FI-90014 University of Oulu, Finland
Acta Univ. Oul. A 463, 2006
Oulu, Finland

Abstract

When implementing their information security solutions organizations have typically focused on technical and procedural security measures. However, from the information systems (IS) point of view, this is not enough: effective IS security requires that users are aware of and use the available security measures as described in their organizations' information security policies and instructions. Otherwise, the usefulness of the security measures is lost.

The research question of this thesis is to explore how IS users' compliance with IS security policies and instructions can be improved. Solving this research question is divided into two steps. Since there is a lack of a comprehensive review of existing IS security awareness approaches, the first step aims at reviewing the existing IS security awareness approaches. This kind of analysis is useful for practitioners as they do not necessarily have the time to go through a large body of literature. For scholars, such an analysis shows what areas of IS security awareness have been studied, and to where the need for future research is of greatest importance.

The second step in this dissertation is to address the shortcomings detected by the analysis by developing three novel design theories for improving IS users' security behavior: (1) IS security awareness training, (2) IS security awareness campaigns, and (3) punishment and reward. These design theories aim to help practitioners to develop their own IS security awareness approaches. Finally, testing of the design theory for IS security awareness training (1) in two action research interventions is described. The results of the interventions suggest that this design theory provides a useful and applicable means for developing a training program in organizations. In addition, the results provide empirically evaluated information regarding the obstacles to user compliance with IS security policies and instructions.

In the action research studies described, the goal was to solve practical problems experienced by the host organizations and to understand them and the results achieved from the viewpoint of theory. Consequently, the results as such can not be generalized, but they are of use in the host organizations in planning and delivering subsequent IS security awareness training programs. In addition, the results are utilizable in similar organizations as a point of departure in planning IS security awareness training programs.

Keywords: information systems security, information systems security - awareness, information systems security - training

Acknowledgements

This dissertation has been carried out in the Department of Information Processing Science, University of Oulu during the years 2003-2006. First of all, I wish to express my sincere gratitude to my supervisor, Professor Mikko Siponen for his inspiring support and counseling whenever called upon during the course of this study. Without his excellent guidance this work could not have reached completion. In particular, he has contributed to the fourth chapter of this dissertation, which is based on an unpublished research paper "Three design theories for IS security awareness" co-authored by Professor Siponen.

I would also like to thank the preliminary examiners of this dissertation, namely Professor Gurpreet Dhillon, School of Business, Department of Information Systems, Virginia Commonwealth University, and Professor Reima Suomi, Department of Management, Information Systems Science, Turku School of Economics and Business Administration, for their insightful comments on the thesis.

I am also grateful to the two host companies of the action research interventions for an inspiring working environment and providing me with the possibility to test my ideas in real organizations. Special thanks go to two skilful IS security professionals, Pasi Koistinen and Paavo Laakso, for fruitful co-operation and interesting and inspiring professional discussions.

My sincerest thanks are due to my family. Before all others, I wish to express my deepest gratitude to my wife Anu for her love and immense support throughout this PhD research process. I also owe my special thanks to our two wonderful daughters, Sanna and Niina. They really have made this world a better place to live.

This research has been financially supported in its different phases by my former employer, Laurea Polytechnic, and by HPY Research Foundation. Without such support, completing the present study would have been much harder.

Contents

1 Introduction

Information security can be defined in terms of confidentiality, integrity and availability (e.g., Parker 1998, Tudor 2002). Today, organizations' information assets are largely in electronic form. This electronic information is processed with the help of information systems (IS), which communicate extensively over private networks and the Internet. An example of this is given by the *Information security breaches 2004 survey*, which points out that about 90 percent of UK businesses send email across the Internet, browse the web and have a web-site (PriceWaterhouseCoopers 2004). The wide use of information systems and the Internet not only by organizations, but also by criminals and IS abusers has led to increased importance of information security considerations (e.g., Straub & Welke 1998, Schlienger & Teufel 2002).

In implementing their information security solutions organizations have typically focused on technical and procedural security measures (Schlienger & Teufel 2002, Stanton, Caldera, Isaac, Stam & Marcinkowski 2003). In the same vein, the existing information security research in general has focused on the technical aspects of information security often ignoring its human dimension (Stanton *et al.* 2003). However, concentrating on technical and procedural aspects of information security alone is inadequate as IS users may not follow technical and procedural information security measures. This is not a desirable situation. If users do not follow security measures the usefulness of these measures is lost (Siponen 2000a p. 31, 2000b p. 197, 2001 p. 26, ∅lnes 1994 p. 632). Consequently, from the IS point of view, effective IS security requires that users are aware of and follow their security mission as described in their organizations' information security policies and instructions.

Recently, the importance of the human factor in IS security have been picked up by both the research community and IS security practitioners (e.g., Parker 1998, 1999, Peltier 2000, Siponen 2000a, 2000b, Straub 1990) with the result that 59 IS security awareness approaches have been put forward by practitioners and scholars. These approaches can be classified into two categories. Studies in *the first category* consider IS security awareness to mean attracting users' attention to IS security issues (e.g., Hansche 2001a, Katsikas 2000). Studies in *the second category* regard IS security awareness as users' understanding of IS security and, optimally, committing to it. As such, users' improved IS security awareness appears as their attitudinal and behavioral changes

causing them to protect information assets (e.g., Beatson 1991, Gaunt 1998, 2000, Hadland 1998, Lafleur 1992, Martins & Eloff 2002, Mitnick 2002). The existing IS security awareness approaches have, however, been criticized for lacking theoretically grounded and testable concrete guidance to ensure that users are committed to fulfilling their IS security mission (e.g., Aytes & Connolly 2003, Siponen 2000a).

1.1 Research question, objective and scope

Given this problem, the research question of this thesis is to explore *how IS users' compliance with IS security policies and instructions can be improved*. Solving this research question is divided into the following two steps. Since there is a lack of a comprehensive review of existing IS security awareness approaches, *the first step* aims at reviewing the existing IS security awareness approaches. This kind of analysis is useful for practitioners as they do not necessarily have the time to go through a large body of literature. For scholars, such an analysis shows what areas of IS security awareness have been studied, and to where the need for future research is greatest. *The second step* aims to address the shortcomings detected by the analysis by developing theoretically grounded and empirically validated IS security awareness approaches.

Research step 1: To examine what approaches are proposed in the existing research to improve users' IS security behavior and their research objectives, theoretical background, research approaches and assumptions about the organizational role of IS security.

Research step 2: To explore how users' security behavior can be improved in practice.

Research step 1: The aim of the first research step is to make sense of the different approaches proposed by the existing research to improve users' IS security behavior. The first goal is to identify IS security awareness approaches that seek to make a concrete impact on IS users' security behavior and to shed light on the organizational role of IS security presented by these approaches. This can help practitioners to choose approaches that fit into the culture and aims of their organization rather than randomly selecting an approach. For example, IS security awareness approaches that consider people purely as a means to ensure security may be unsuitable for an organizational culture that regards user autonomy as an important value.

The second aim of the first research step is to contribute to the understanding of the theoretical background of the existing IS security awareness approaches. This is useful for both scholars and practitioners, as understanding the theoretical background extends their knowledge of why a particular IS security awareness approach has (or is expected to have) the desired impact on users' security behavior. In addition, the need to use appropriate theories in the IS discipline has been pointed out by scholars (e.g., Walls, Widmeyer & El Sawy 1992).

The third goal of the first research step is to point out to what extent IS security awareness approaches incorporate empirical evidence on their practical effectiveness. Eliciting such information will benefit practitioners, since approaches based on empirical evidence can be considered more credible in terms of their practical usefulness and efficiency than approaches lacking such evidence.

Research step 2: As earlier stated identifying the theoretical background of existing IS awareness approaches benefits both scholars and practitioners. In addition, IS security practitioners would benefit from concrete guidance on how to implement the approaches in their organizations. Furthermore, presenting testable research agendas for IS security awareness approaches would be beneficial for scholars by identifying issues for further exploration. However, it has been pointed out by Aytes and Connolly (2003) and Siponen (2000a) that the existing IS security awareness approaches lack theoretically grounded and testable concrete guidance to ensure that users are committed to fulfilling their IS security mission. Consequently, the first aim of the second research step is to explore how the aforementioned concerns can be addressed. Finally, the second goal of the second research step is to design approaches that address those concerns and to test the approaches in practice.

1.2 Research strategy

This dissertation employs conceptual-analytical, constructive, and theory-testing research approaches (Järvinen 1997, 2000, see Table 1). The first research step employs conceptual analysis. Also the second research step utilizes conceptual analysis to identify the theoretical background and proposed research agendas of existing IS security awareness approaches. In addition, constructive research with a theory-testing research approach is employed. Constructive research is applied to construct three novel, theory-based IS security awareness approaches and theory-testing research is applied to test one of them in practice. With respect to testing of the new approach, action research was the selected research method. In action research, the problem to be explored is diagnosed, a plan of action is developed, the plan is implemented, data is collected and evaluated, and the findings of the investigation are reflected on (Baskerville 1999).

Table 1. Research strategy: research approaches for solving the research question.

Research step	Chapters	Research approaches
What approaches are proposed in the existing research to improve users' IS security behavior and what are their research objectives, theoretical background, research approaches, and assumptions about the organizational role of IS security?	II, III, IV	Conceptual analysis
How can users' security behavior be improved in practice?	IV, V	Conceptual analysis, constructive research, and theory testing with action research

It has been argued that action research is ideal for studying information system methods in a practical setting (Baskerville & Wood-Harper 1996, 1998) and empirically studying the applicability of the proposed new solution in practice. Action research was also chosen as the research methodology in the second research step of this dissertation. Action research is a form of field intervention that aims at solving practical, real problems faced by an organization. Hence, it is an empirical method that is practical. In

addition, it is interventionist, iterative, participatory, clinical, qualitative, interpretive, and critical (cf., Baskerville & Wood-Harper 1996, 1998, Carr & Kemmis 1986, Kemmis & Wilkinson 1998). Action research does not aim at finding general or universal mechanistic-causal laws. Rather, it aims at finding systematic actions that can be taken to resolve specific problems in practice (Stinger 1999 p. 17), at the same time validating theories through their successful use.

Baskerville and Wood-Harper (1998) have proposed seven validity criteria for information systems 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 intervenes in the research setting; (4) the method of data collection includes participatory observation; (5) changes in the social setting are 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. The aforementioned criteria are applied when evaluating the results of the interventions.

1.3 Structure of the thesis

The rest of this thesis is organized as follows. The second chapter presents an overview of existing IS security awareness approaches. The third chapter reviews these approaches by analyzing them from the following three viewpoints: (1) the organizational role of IS security, (2) research objectives and (3) the research approach employed and theoretical background. As a result, a critical analysis of the existing IS security awareness approaches is presented.

The fourth chapter proposes three IS security awareness approaches following the idea of design theorizing: (1) IS security awareness training, (2) IS security awareness campaigns, and (3) punishment and reward. It is based on an unpublished research paper *"Three design theories for IS security awareness"* (Puhakainen & Siponen 2005). The fifth chapter explores the design theory for IS security awareness training empirically through the aid of action research. The empirical exploration is conducted within two companies. In the sixth chapter, the limitations and implications of this dissertation are discussed and the seventh chapter summarizes the key findings.

2 An overview of existing IS security awareness approaches

2.1 Determining the source material for the literature review

A complete review of the literature should cover all relevant literature on the topic without being confined to one research methodology, one set of journals or one geographic region (Webster & Watson 2002 p. xv-xvi). Sharing this viewpoint, the literature review presented in the second and third chapters of this dissertation aims to cover all existing IS security awareness approaches. To achieve this aim, the following process was employed to determine the source material for the review. First, IS and information security journals were explored through the aid of digital databases (e.g., ACM Digital Library, EBSCO, Elsevier Science Direct, Emerald Library, IEEE/IEE Electronic Library, Springer Link) and also directly scanning the journals' tables of contents. In addition, conference proceedings (e.g., International Conference on Information Systems, Americas Conference on Information Systems, IFIP International Conference on Information Security, IFIP International Conference on IS security, Hawaii International Conference on System Sciences, Information Security Curriculum Development) were examined directly and by utilizing the aforementioned electronic databases. Finally, the contents of over 300 IS security textbooks were explored. The aforementioned process identified 59 IS security awareness approaches; these are introduced next (see Table 2).

Table 2. Summary of the source material for the literature review.

Study	Source	Study	Source
Aytes and Connolly (2003)	Proceedings of the Ninth Americas Conference on Information Systems	NIST (1996)	National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
Banerjee, Cronan and Jones (1998)	MIS Quarterly, Vol. 22, No. 1	NIST (1998)	National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
Barman (2002)	IS security Policies, New Riders Publishing	NIST (2003)	National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
Beatson (1991)	Proceedings of the Sixth IFIP International Conference on Computer Security	Parker (1998, 1999)	Computer Security Journal, Vol. 15, No. 4; A new Framework for Protecting Information, John Wiley & Sons, USA.
Bray (2002)	Information system security, Vol. 11, No. 1	Peltier (2000, 2002)	Computer Security Journal, Vol. 16, No. 2; IS security Policies, Procedures, and Standards. Guidelines for Effective IS security Management, Auerbach Publications
Cox, Connolly and Currall (2001)	VINE, Issue 123	Perry (1985)	Strategies for Computer Security, Butterworth Publishers
Denning (1999)	Information Warfare and Security, ACM Press	Pipkin (2000)	IS security: Protecting the Global Enterprise, Hewlett-Packard Professional Books, Prentice Hall PTR
Desman (2002)	Building an IS security Awareness Program, Auerbach Publications	Proctor and Byrnes (2002)	The Secured Enterprise: Protecting Your Information Assets, Prentice Hall
Forcht, Pierson and Bauman (1988)	Proceedings of the ACM SIGCPR conference on management of information systems personnel	Rudolph, Warshawsky and Numkin (2002)	Computer Security Handbook, Fourth Edition, John Wiley & Sons, USA

Study	Source	Study	Source
Furnell, Gennatou and Dowland (2001, 2002)	2nd AISM Workshop, International Journal of Logistics Information Management, Vol. 15, No. 5	Sasse, Brostoff and Weirich (2001)	BT technology journal, Vol. 19, No. 3
Furnell, Sanders and Warren (1997)	Proceedings of Medical Informatics Europe '97	Schlienger and Teufel (2002)	Proceedings of IFIP TC11, 17th International Conference on Information Security, Security in the Information Society: Visions and Perspectives
Gaunt (1998)	International Journal of Medical Informatics, Vol. 49, No. 1	Siponen (2000a)	Information Management & Computer Security, Vol. 8, No. 1
Gaunt (2000)	International Journal of Medical Informatics, Vol. 60, No. 2	Siponen (2000c)	Proceedings of IS security for Global Information Infrastructures, IFIP TC11 Fifteenth Annual Working Conference on IS security
Hadland (1998)	Proceedings of New Networks, Old Information: UKOLUG98, UKOLUG's 20th Birthday Conference 1998	Spurling (1995)	Information Management & Computer Security, Vol. 3, No. 2
Hansche (2001a)	Information System Security, Vol. 10, Issue 1	Stacey (1996)	Information System Security, Vol. 5, Issue 2
Hansche (2001b)	Information System Security, Vol. 10, Issue 3	Straub (1990)	Information Systems Research, Vol. 1, No 3
ISF (2005)	International Security Forum (ISF), http://www.isfsecuritystandard.com/index_ie.htm	Straub, Carlson and Jones (1993)	Journal of Management Systems, vol. 5, No. 1
ISO (2005)	International Organization for Standardization (ISO)	Straub and Welke (1998)	MIS Quarterly, Vol. 22, No. 4
Kabay (2002)	Computer Security Handbook, Fourth Edition, John Wiley & Sons	SSE-CMM (1999)	Systems Security Engineering - Capability Maturity Model http://www.sse-cmm.org/model/images/ssecmmv2final.pdf
Kajava and Siponen (1997)	Proceedings of IFIP-TC 11, 13th International Conference on IS security: IS security Management - The Future	Telders (1991)	Computer Security Journal, Vol. 7, No. 2

Study	Source	Study	Source
Katsikas (2000)	International Journal of Medical Informatics, Vol. 60, No. 2	I^2SF (1999)	MIT Information Services and Technology (IST) http://web.mit.edu/security/www/gassp1.html
Kluge (1998)	International Journal of Medical Informatics, Vol. 49, Issue 1	Thomson and von Solms (1997)	Proceedings of the WG 11.2 and WG 11.1 of the TC11 IFIP
Kovacich (1998)	Information system security Officer's Guide: Establishing and Managing an Information Protection Program, Butterworth-Heinemann	Thomson and von Solms (1998)	Information Management & Computer Security, Vol. 6, No 4
Kovacich and Halibozek (2003)	The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program, Butterworth-Heinemann	Tudor (2001)	IS security Architecture, An Integrated Approach to Security in the Organization, Auerbach Publications
Lafleur (1992)	Computer Control Quarterly, Vol. 10, No. 4	Vroom and von Solms (2002)	Proceedings of IFIP TC11 17th International Conference on IS security
Markey (1989)	Proceedings of the Fifth IFIP International Conference	Vyskoc and Fibikova (2001)	Proceedings of the IFIP WG 9.6/11.7 Working-Conference
Martins and Eloff (2002)	Proceedings of IFIP TC11 17th International Conference on IS Security	White House (2003a, 2003b)	White House www.whitehouse.gov/pcipb/priority_3.pdf; http://www.whitehouse.gov/pcipb/appendix.pdf
McLean (1992)	Proceedings of Eighth International Conference on IS security	Wood (2002)	Computer Security Journal, Winter 2002, Vol. 18, No. 1
Mitnick (2002)	The Art of Deception: Controlling the Human Element of Security, Wiley Publishing	Wood (1995)	Computer Fraud & Security Bulletin, June 1995
Murray (1991)	Proceedings of the IFIP TC11 Seventh International Conference on IS security		

2.2 An overview of existing IS security awareness approaches

Aytes and Connolly (2003) present a model of user behavior that emphasizes the factors relating to the user's perception of risk and the choice based on that perception. In this model, information sources (e.g., training, media, coworkers, friends, policies, procedures and personal experience) provide information that forms the user's knowledge (e.g., about threats and vulnerabilities, awareness of countermeasures, potential consequences to self and others and the costs of secure behavior). This information must be perceived by the user to be relevant in his situation. The user's perceptions (availability and usability of safe practices, probability of negative consequences, significance of negative consequences, ease of recovery and beliefs regarding peer behavior) therefore represent an important factor in the behavioral choice process that leads to the actual behavior associated with the choice (i.e., to use or not use the countermeasure). The behavior results in an outcome, either positive or negative that is fed back as a source of new information.

Banerjee, Cronan and Jones (1998) identify situational characteristics which exert an impact on the ethical behavior-related intention of IS employees when they are faced with ethical dilemmas. The results of the study indicate that an IS employee's intention to behave ethically or unethically is strongly related to the context of the individual's perceived organizational environment and influenced by that individual's moral obligation toward performing an act. Consequently, the study proposes that companies should make their ethical policy clear to their employees and ensure that strong deterrents are in place (Banerjee *et al*. p. 49).

The goal of Barman (2002) is to provide an example of the process of writing and implementing organizational IS security policies. To succeed in implementing such a process, he emphasizes the importance of security awareness training (Barman 2002 p. 32). The training should aim to teach the organizational IS security policy to employees. In addition, it should emphasize employees' role in adhering to the policy.

Beatson (1991) discusses how to avoid security breaches. For this purpose, the study suggests the principle of least possible privilege, psychological profiling of potential new employees, division of responsibilities, clear data classification rules, and enforced security policies by creating and maintaining a high level of IS security awareness. This is achieved through the appropriate training of employees.

Bray (2002) argues that companies are especially vulnerable to security breaches when significant changes occur, such as a reduction in the workforce. As a means to avoid security breaches during organizational changes the study suggests a program of IS security awareness training that covers e.g., social engineering, speaking with the press, password protection, encouraging administrators to be vigilant when reviewing system and security logs, and combining heightened computer and security alertness with heightened physical security alertness.

Cox, Connolly and Currall (2001) argue that user behavior is critical to IS security. For this reason, the study examines three approaches which can have an impact on IS users' behavior in an academic setting: (1) a discussion session, (2) a checklist, and (3) a web based tutorial. The results of the study point out all three IS security awareness

approaches seemed to be valid in raising users' awareness generally, but also to support the introduction of relatively novel technologies such as the encryption of email.

Denning (1999) argues that training (education) is an important part of defensive information warfare and proposes IS security awareness training programs as a means to inform employees with respect to security policies, make them aware of the risks and potential losses, and teach them the proper utilization of IS security practices and technologies.

Desman (2002) presents a program that aims to raise users' IS security awareness. The program contains the following four stages: (1) getting started (discovering the current situation and how it is possible to leverage existing resources in order to build a program), (2) establishing a baseline: building up 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.

Forcht, Pierson and Bauman (1988) discuss the importance of ethical awareness for IS security and emphasize the role of people, their attitudes, actions and sense of right and wrong in addressing IS security issues. The study proposes that by building a strong base in terms of ethical awareness and constantly reiterating the necessity to maintain this base organizations can increase their IS security. The study suggests IS security awareness programs as a potential means to achieve this outcome.

Furnell, Gennatou and Dowland (2001, 2002) present a prototype tool for IS security awareness training. The tool is meant for employees to pursue self-packed security training by providing an environment that permits them to simulate the introduction of security measures in a number of pre-defined case study scenarios. According to Furnell *et al.* (2001, 2002), this familiarizes employees with the types of countermeasures available, the situations in which they are suitable and any constraints that they may impose. The tool is expected to be particularly useful in small organizations where specialist knowledge is scarce and issues need to be addressed by existing employees.

Furnell, Sanders and Warren (1997) discuss the need to promote IS security issues within healthcare establishments. They argue that promoting IS security in organizations requires IS security awareness training. The study highlights issues that a healthcare establishment (HCE) should address in setting up a training program. These issues include covering employees' day-to-day duties, training for the use of systems and applications, training in specific issues (e.g., new viruses), segmenting audiences properly (e.g., new employees, existing personnel, specialists like IT and security staff), and defining clear responsibilities over developing and delivering the training program. Furnell *et al.* (1997) also propose that all staff should be aware of disciplinary action resulting from non-compliance with the organization's IS procedures.

Gaunt (1998) presents a case study in the healthcare environment of the development and implementation of an IS security policy. In the study, an IS security awareness program was launched to overcome users' lack of IS security awareness and the unwillingness to take responsibility for security issues. Gaunt (1998) argues that implementing an organizational IS security policy requires that the policy should incorporate clear definitions of user responsibilities for IS security. In addition, the terms and conditions of employment should require compliance with the policy and the policy should regularly be trained to all employees.

Gaunt (2000) discusses practical approaches for creating a security culture in the health care environment. He argues (Gaunt 2000 p. 152) that the most significant threat to the security of information in an organization is its staff. For this reason, the attitude of employees' plays a key role in good IS security. Hence, all employees should be aware of, agree with and observe procedures aimed at preserving security of information. Gaunt (2000 p. 154) also argues that the most important influence on staff attitude is a demonstration of the commitment to security by key opinion formers. In addition, he presents that user participation in the development of an organizational IS security policy is necessary if it is to achieve wide acceptance.

Hadland (1998) discusses raising Barclays Bank's employees' awareness of the existing IS security practices (accountability, access to systems, viruses, the use of FAX and email, unauthorized software, portable PCs, backups, and physical security). The aim was to ensure that employees follow these practices and training was the means selected to achieve this outcome. The training utilized a video drama, presentation and discussion built around the drama (Hadland 1998 p. 94). In addition, leaflets were used as supportive material.

Hansche (2001a) deals with developing and implementing an organizational IS security awareness program. The goal of the program is to heighten the importance of IS security through the following five stages: (1) setting the goal for the program, (2) deciding on the content of the program, (3) selecting delivery options, (4) implementation (as well as overcoming obstacles), and (5) evaluation of the program.

Hansche (2001b) presents a framework for an IS security training program. The purpose of the program is to build knowledge, skills and abilities which facilitate job capabilities and performance. The framework contains the following phases: (1) establishing training needs and setting up the learning objectives, (2) developing the program plan to basis of the learning objectives, (3) training design and development (instructional strategy), (4) implementation, and (5) evaluation of the program.

Information Security Forum's standard (ISF 2005), "*The Forum's Standard of Good Practice for IS security, January 2005*" seeks to address IS security from a business perspective. It deals with security measures that should be used for controlling risks associated with organizations' critical information systems and puts forward several IS security measures for this purpose. According to the standard, IS security awareness is a one of these critical security measures and it should be high among all employees who have access to the information and systems of the organization. Consequently, the standard argues for the importance IS security awareness training and printed IS security awareness material such as brochures, posters and electronic material.

ISO/IEC standard 17799:2005 (second edition), *"Information technology - Code of practice for IS security management"* (ISO 2005 p. 26) argues that all employees should receive job-relevant awareness training in and regular updates on organizational IS security policies and procedures. The standard recommends that IS security awareness training is used to introduce new employees the organization's security policies and expectations before access to information or services is granted. Furthermore, it claims that ongoing training should include security requirements, legal responsibilities and business controls, correct use of information processing facilities (e.g., log-on procedure, use of software packages) and information on the disciplinary process for employees who have committed a security breach.

Kabay (2002) reviews the principles of social psychology as a means to improve IS system users' security behavior. The study aims to add to understanding of the behavior of people from the perspective of social psychology. In addition, it suggests ways to make people more receptive to IS security policies and to change their beliefs and attitudes in a manner more positive toward IS security. Finally, Kabay (2000) explores how social psychology can be used in groups in order to improve success rates with respect to IS security policies.

Kajava and Siponen (1997) discuss impacting on IS users' security behavior within the context of a Finnish university. The IS security awareness approaches used for this purpose were student education, end-user training and IS security awareness training for IS specialists. In addition, the study underlines the commitment of management as an important factor impacting on users' IS security awareness.

Katsikas (2000) discusses the importance of management's knowledge with regard to IS security issues. The study argues for training in order to increase management's knowledge and presents a methodology for determining IS security training needs within healthcare establishments. In the methodology, learning is presented as evolving on three knowledge levels: (1) awareness, (2) training, and (3) education. Awareness (1) activities aim at attracting employees' attention. The goal of training (2) is to produce security skills for employees, who need special knowledge. Education (3) aims at creating the expertise necessary for IS security specialists and managers.

Kluge (1998) argues that model codes of ethics make health information professionals (HIPs) aware that ethical behavior is necessary to protect their patients' confidential electronic information. In addition, Kluge (1998) sketches a model code of ethics, which presents ethical principles for HIPs.

Kovacich (1998 p. 113-116) describes an example of an IS security awareness program. The program has two parts: (1) awareness briefings (e.g., training sessions) and (2) continuing awareness material (i.e., printed material). The purpose of the awareness briefings is to provide information necessary for protecting information and information systems and they are tailored to specific audiences (e.g., new employees, managers, system users, IS specialists, manufacturing, accounting and finance, procurement, HR department, security personnel). Moreover, the purpose of the printed awareness material is to remind constantly all employees of IS security issues.

Kovacich and Halibozek (2003 p. 247-272) discuss implementing a security awareness training program as part of the corporate asset protection program. The security awareness program aims to make the target audience aware of the need for asset protection practices, specific asset protection requirements, what unauthorized actions are with respect to asset protection and appropriate violation-reporting procedures. Kovacich and Halibozek (2003) propose that such training should be delivered through briefings (e.g., training sessions) and continuing awareness material (i.e., printed material) such as posters and booklets.

Lafleur (1992) discusses ways in which employees' resistance to more secure behavior can be overcome. He suggests an IS security awareness program for this purpose. According to Lafleur (1992 p. 4), an IS security awareness program requires two techniques: (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.

Markey (1989) presents a practical example of an IS security awareness program used by the US Department of State to raise security awareness on the part of all employees. The program consists of the following components: a briefing for top management, seminars for employees responsible for security at overseas locations and IS security briefings for new employees.

Martins and Eloff (2002) present a model for implementing and enhancing the culture of IS security. Their model focuses on three levels of organizational behavior (Martins & Eloff 2002 p. 206-210): the organizational level, group level and individual level. Accordingly, an organization's IS security culture must be improved by taking human behavior into account. Consequently, Martins and Eloff (2002) suggest that each employee should be informed through IS security awareness training to act according to what is expected of him in order to protect information assets.

McLean (1992) discusses using basic marketing concepts in designing an IS security awareness program. He argues that an IS security awareness program targets the attempt to change people's values, perceptions and behavior. According to him, this goal can be achieved by using campaigns having the following five stages: (1) planning and preparation, (2) production, (3) initial conditioning, (4) behavioral change, and (5) an ongoing program.

Mitnick (2002 p. 249-258) argues for an ongoing IS security awareness training program as a means to resist social engineering. According to him, the goal of training programs is to influence people to change their behavior and attitudes by motivating employees to protect the information assets of the company. According to Mitnick (2002 p. 250), the program must reach all employees, but it must also be customized to the specific requirements of several different groups within the organization. He also argues that top management must show real commitment to the program as otherwise it is difficult to motivate the employees. Mitnick (2002) suggest the following means to deliver an IS security awareness 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. He also argues for rewards and punishment to support the results of the IS security awareness training program.

Murray (1991) outlines some of the problems associated with poor IS security. He argues that the biggest security problems result from the incompetence of employees who do not understand the dangers inherent in their actions (Murray 1991 p. 204). He emphasizes the need for an organizational IS security awareness program to overcome this problem. Accordingly, this kind of a program should be a combination of courses, seminars, videos, handouts, directives, reminders and newsletters. In addition, management's support for and commitment into the program is vital for its practical efficiency.

The document *"An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12"* suggests the following seven-step approach for developing a IS security awareness training program (NIST 1996 p. 150): (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.

The document *"Information Technology Security Training Requirements: A Role- and Performance-Based Model, NIST Special Publication 800-16"* (NIST 1998) presents a conceptual framework for providing information technology security training. The study argues that over time, employees acquire different roles relative to the use of information systems. Consequently, their need for security training changes according to those roles. For this reason, the framework segments an employee's organizational role into six functional specialties: (1) manage, (2) acquire, (3) design and develop, (4) implement and operate, (5) review and evaluate, and (6) use. Furthermore, the study proposes three fundamental training content categories for consideration: (I) knowledge of laws and regulations, (II) security program and (III) system life cycle security. An employee's training needs in each of the three areas (I-III) are determined by his functional specialties (1-6) as defined by his organizational role.

The document *"Building an Information Technology Security Awareness and Training Program, NIST Special Publication 800-50"* (NIST 2003) aims to provide guidance for building an effective information technology security program. The guidance is presented in the form of a life-cycle approach. Consequently, the document puts forward four critical steps in the life cycle of an IT security awareness and training program: (1) awareness and training program design, (2) awareness and training material development, (3) program implementation and (4) post-implementation. The document offers guidance on (I) identifying training needs; (II) developing a training plan, (III) obtaining funding to the training program (IV) selecting training topics, (V) finding sources of training material; (IV) implementing training material using a variety of methods; (VII) evaluating the effectiveness of the program, and (VIII) updating and improving the focus of the program.

Parker (1998, 1999) proposes that the primary motivation for IS security must come from rewards and penalties directly associated with job performance. He also claims that conflicts between job performance and security constraints must be removed by making security a part of job performance. Furthermore, Parker (1998, 1999) puts forward six factors for good IS security: (1) support from top management, (2) support from human resources, (3) job descriptions that include specific assignments to protect and be accountable for information and systems, (4) evaluations and discussions of the employees' support for, and practice of, IS security in annual job performance appraisals, (5) documenting and broadcasting security efforts and rewards given, and (6) motivating managers to ensure their support for IS security.

The studies by Peltier (2000, 2002) present an IS security awareness program having the following stages: (1) segmenting the audience, (2) establishing the roles expected of employees, and (3) delivering the message. The goal of the program is to stress how security will support the business objectives of the company and raise the consciousness of employees in ways which protect information and information processing resources. 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.

Perry (1985 p. 92) argues that enthusiasm for security is a behavioral change which can be expressed by utilizing the following formula: *Behavior = individual + environment.* According to Perry (1985), changing either of the two variables will change behavior. The key to changing the environmental attitude about security is to make it

important. He calls the principle behind this as *"the hammer theory*." This principle holds that when a new concept is properly introduced in the organization, employees will be keen on using it (Perry 1985 p. 94). Perry (1985 p. 94-95) suggests the following means to increase the importance of IS security: 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, and issuing an IS security policy. He also proposes some means to increase employees' (individuals') enthusiasm for IS security: downloading IS security tasks, individual ownership of IS security, feedback on effectiveness of IS security tasks, a reward system, variety in performance of IS security activities, and personal mastery of IS security responsibilities.

Pipkin (2000 p. 103) argues that an IS security awareness program is the first step in an organizational IS security program. According to him, the awareness program must be targeted at all employees and it must be a continuous effort. He presents several methods for delivering the program: web sites, log-on messages, banners, newsletters, posters, trinkets (e.g., pens, mouse pads, coffee mugs), organizational meetings, and personal employee review sessions.

Proctor and Byrnes (2002) claim that the central component of an organizational IS security is an IS security awareness program that aims to improve employees' behavior. They suggest that an IS security awareness program can be delivered through the aid of IS security awareness training which utilizes basic marketing techniques.

Rudolph, Warshawsky and Numkin (2002) sketch an IS security awareness training program, which targets employees' security behavior. They propose that the program can be implemented as a media campaign covering the following issues: risks related to IS security, basic IS security measures and their use, employees' IS security responsibilities, and IS security incident reporting. They propose several tools and 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, suggestion programs, contests, IS security audits, various events, briefings, conferences, and presentations.

Sasse, Brostoff and Weirich (2001) examine the issues involved in security design, including characteristics of the technology and users, users' goals and tasks, the working context and how human/computer interaction can be used to address these issues. According to them, users must have knowledge of security issues and they must be motivated to use security measures. In addition, security mechanisms must be matched to users' capabilities and tasks. They also suggest that the context as well as both the physical environment and the social and organizational environment must create the motivation for security. As a possible means to increase users' knowledge and motivate them, Sasse *et al.* (2001) propose the use of training, punishment and reporting security-related incidents.

Schlienger and Teufel (2002) propose a socio-cultural approach to IS security and explain how the cultural theory can help to increase the overall security of an organization. According to them, the layers of security culture are represented by (1) corporate policies, (2) top management, and (3) individuals. The individual level (3) covers employees' IS security awareness. Schlienger and Teufel (2002) suggest that the most important points concerning security culture are the exemplary behavior of

managers, security training of employees, and the rewarding of behavior which conforms to security practices.

Siponen (2000a) argues that IS security awareness programs should be grounded upon behavioral theories and, e.g., provide users with answers as why following security guidelines is necessary. The aim of such a program should be to achieving a situation where users' internalize and follow IS security policies. In this respect, Siponen (2000a) presents a framework for persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions.

Siponen (2000c) proposes that human morality exerts a role in terms of security. He proposes ethical education to improve employees' IS security behavior. According to Siponen, this should be done first by selecting a suitable ethical principle (e.g., the veil of ignorance by Rawls 1999) and then justifying the principle to the listeners (i.e., why the chosen principle is the best possible for the situation). Next the selected principle should be used to justify claims that certain IS security acts are morally acceptable or favored.

Spurling (1995) discusses promoting security awareness and users' commitment to IS security. He argues that users' commitment to security requires a process that fits into the culture of the organization and presents a case study in which a company based its IS security awareness efforts on three principles: (1) high quality of all IS security work, (2) involving people, and (3) constantly reminding people about IS security issues. In the example organization, the following means were used to emphasize the importance of IS security to the employees: presentations and training, involvement, work instructions, email messages, booklets, newsletters, screen savers and a problem-reporting system.

Stacey (1996) presents a tool for evaluating the maturity of an organization from the perspective of IS security. The tool – the IS security program maturity grid – is composed of five stages of maturity (uncertainty, awakening, enlightenment, wisdom, benevolence) as well as five measurement categories (management understanding and attitude, security organization status, incident handling, security economics, security improvement actions). *Uncertainty* is descriptive of management's total lack of understanding with respect to IS security. Upon *awakening* to these matters, management understands that IS security engineering may be valuable. However, IS security is based on past threats, and it is not understood why security problems exist. Achieving *enlightenment* requires IS security awareness with regard to the training of users. The organization understands the importance of IS security and it seeks solutions to prevent incidents, but when incidents occur they are noticed and reported. *Wisdom* requires that management must actively attend IS security awareness training and obtain an understanding of the necessary matters connected with IS security engineering. In addition, all employees must be well aware of IS security issues.

Straub (1990) investigates whether a management decision to invest in IS security enhances the control of computer abuse and suggests (Straub 1990 p. 19) that publicly known efforts to detect abuse may significantly deter abusive behavior. Consequently, he proposes the following actions be taken: (1) policies regarding proper and improper use of information systems need to be established. (2) IS security officers should inform and train IS users about acceptable system use, (3) IS security officers should strengthen IS security efforts by such methods as assigning and monitoring passwords, classification of information and programs by security level, and surveillance of suspicious activities in

the system, and (4) IS security officers should consider implementation of software preventives (e.g., RACF, Top Secret).

Straub, Carlson and Jones (1993) present a field experiment designed to test how student cheating during a computer programming assignment can be deterred. The implications of the study for business settings suggest that in order to deter computer abuse, managers should encourage employees to engage in the proper use of systems. For this, they can use formal and informal meetings, employee orientation sessions, and training sessions. Besides emphasizing ethical use, managers should also stress that violations of company policies will meet with sanctions. In addition, they should implement tools which automatically detect possible computer abuses.

Straub and Welke (1998) present a theory-based IS security program that aims to make managers aware of the full range of actions they can take to reduce IS security risks. The program includes (1) use of a security risk planning model, (2) IS security awareness training, and (3) countermeasure matrix analysis. Straub and Welke (1998) argue that IS security actions can deter potential computer abusers from committing acts which violate organizational policies. IS security awareness programs are important in this respect, as educating employees and managers increases knowledge with regard to risks and emphasizes actions like policies and sanctions for violators (Straub & Welke 1998 p. 445). According to Straub and Welke (1998 p. 445), a major reason for awareness training is to convince potential abusers that the company is serious in protecting its information assets, and that violators will be punished. Furthermore, Straub and Welke (1998) provide evidence that practitioners are willing and able to adopt theory-based tools for security planning.

The document "*Systems Security Engineering - Capability Maturity Model SSE-CMM, Model Description Document V. 2.0, April 1, 1999*" (SSE-CMM 1999) presents a process reference model focused on the requirements for implementing security in a system. It aims to describe the essential characteristics of an organization's security engineering process by capturing practices generally observed in industry. SSE-CMM (1999) has two dimensions, (1) domain and (2) capability. The *domain dimension* consists of all the practices that collectively define security engineering. The practices related to the domain dimension are called *base practices*. The *capability dimension* represents practices that indicate capability for process management and institutionalization. These practices are called *generic practices* as they apply across a wide range of domains. The base practice BP.01.03 deals with IS security awareness training: *"Manage security awareness, training, and education programs for all users and administrators"* (SSE-CMM 1991 p. 171). It emphasizes that IS security awareness training requires management in the same way as other training efforts. It also gives the following examples: user review of security training material, logs of all training undertaken and the results of the training, periodic reassessments of the user community level of knowledge with regard to security, and records of training material. In addition, the following base practices related to ongoing skills and knowledge are applicable to IS security awareness training (SSE-CMM, 1999, p. 281-290): (BP.21.01) identify training needs, (BP.21.02.2) select the mode of knowledge or skill acquisition, (BP.21.03) assure availability of skill and knowledge, (BP.21.04) prepare training materials, (BP.21.05) train personnel, (BP.21.06) assess training effectiveness, (BP.21.07) maintain training records, and (BP.21.08) maintain training materials.

Telders (1991) explains how IS security awareness can be developed and implemented through the following five-step IS security awareness program (Telders 1991 p. 61): (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.

The document *"The International IS security Foundation, Generally Accepted System Security Principles, (GASSP) Version 2.0",* I^2SF (1999), relates to physical, technical and administrative IS security. It encompasses pervasive, broad functional and detailed security principles. *Pervasive principles* provide general guidance to establish and maintain the security of information. They form the basis of broad functional principles and detailed principles. Pervasive principles are few in number and rarely change. *Broad functional principles* are subordinate to one or more of the pervasive principles. They are more numerous and specific. In addition, they guide the development of more detailed principles, and change only when reflecting major technical developments or other high-impact issues. *Detailed principles* are subordinate to one or more of the broad functional principles. They are numerous, specific and they change frequently as technology and other affecting issues evolve. IS security awareness is included in both pervasive and broad functional principles. The pervasive principle, *the Awareness Principle* (2.1.2), states that *"all parties with a need to know should have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information."* The broad functional principle, *Education and Awareness* (2.2.2), states that *"management shall communicate IS security policy to all personnel and ensure that all are appropriately aware. Education shall include standards, baselines, procedures, guidelines, responsibilities, related enforcement measure, and consequences of failure to comply."*

Thomson and von Solms (1997) propose an organizational IS security awareness program. The program aims at making all users and parties responsible for information aware of its value and importance. In addition, the program aims to make users aware of the security procedures that they are supposed to be following. Thomson and von Solms (1997) identify three different target groups for such a program: top management, information systems management, and end-users. They propose the following means to deliver the program (Thomson & von Solms 1997 p. 102): presentations, workshops and continuing material such as booklets, newsletters, multi-media packages, e-mail remainders and screen savers.

Thomson and von Solms (1998) argue for the importance of employees' IS security awareness training in order to protect an organization's information assets. They propose a variety of principles drawn from social psychology (operant learning, shaping, social learning, conformity, obedience, reciprocity, commitment, attribution, self-persuasion, dissonance, exposure, attention, acceptance, shaping, instrumental learning, retention) be deployed to improve the practical efficiency of IS security awareness training.

Tudor (2001) discusses the design and implementation of a holistic IS security architecture incorporating the following five components: (1) security organization and infrastructure, (2) security policies, standards and procedures, (3) security baselines and risk assessment (4) security awareness and training programs, and (5) compliance. Tudor

claims that awareness and training are its most significant elements, and consequently presents a ten-phase plan for a security awareness and training program (Tudor 2001 p. 161-162): (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.

Vroom and von Solms (2002) present an IS security awareness program. The program aims at informing users of the procedures and controls which are in place to secure information. They identify three different target groups for an IS security awareness program: end-users, information technology (IT) personnel and top management (see also Thomson & von Solms 1998). Vroom and von Solms (2002) propose a model for an IS security awareness program embodying the following seven steps (Vroom & von Solms 2002 p. 31-32): (1) educating top management in 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.

Vyskoc and Fibikova (2001) present the results of a survey with the purpose of evaluating what IS system users think about IS security issues. They also compared the results with the expectations of IS security specialists. It turned out that there is a gap between the reality and the expectations of specialists. The results of the survey aim to point out these differences and help to target the effort of managers and specialists to influence users' behavior and attitudes towards creating a better security culture. For this purpose, they suggest unnamed management techniques.

The document *"White House: The National Strategy to Secure Cyberspace, Priority III: A National Cyberspace Security Awareness and Training Program"* (White House 2003a) describes a program developed by the US government to promote a national IS security awareness program and to ensure security training and education programs necessary to the protection of the nationwide information technology infrastructure. The components of the program are: (1) awareness of home users, small businesses, large enterprises, institutions of higher education, private sectors, state and local government, (2) fostering adequate training and education and increasing the efficiency of existing federal training programs, and (3) promoting private sector support for well-coordinated, widely recognized professional certifications. In addition, the document *"White House: The National Strategy to Secure Cyberspace, Appendix: Actions and Recommendations (A/R) Summary."* (White House 2003b) offers several actions and recommendations that may be taken concerning a national IS security awareness and training program, including awareness campaigns, securing networks, the training of IS security professionals, federal IS security training programs, and the development of security certification programs.

Wood (2002 p. 16) argues that in many cases, human actions undo technical IS security measures. Consequently, organizations must make serious efforts to educate

users and evaluate whether they are in compliance with the organization's IS security policies and instructions on an ongoing basis. To enhance such efforts, Wood (2002) describes a security education campaign, *"Human Firewall"*, which is an international effort aimed at helping managers and employees in organizations to change attitudes and behavior towards the improvement of protection for critical information assets. He proposes the following plan of actions for this purpose: (1) Join the campaign by signing the Human Firewall Manifesto at the campaign's web site, (2) perform a benchmark survey on the campaign's web site, (3) use the results of the survey to highlight your organization's security needs, (4) propose that your organization should perform a risk assessment, (5) on the basis of the risk assessment, discuss how users' IS security awareness should be improved in your organization, (6) evaluate the adequacy of your organization's IS security resources (e.g., policies, budget, staff), and (7) train users through the aid of an ongoing program and measure the results.

Wood (1995) lists 53 IS security awareness approaches classified by the type of communication involved: in person (e.g. training, video conferences), in writing (e.g., security manual, posters, notices on paper), electronic (e.g., computer-based training, log-on messages), and other (e.g., security reminder messages on coffee mugs).

3 Analysis of existing IS security awareness approaches

In this chapter, the existing IS security awareness approaches are explored from the following three viewpoints: (1) the organizational role of IS security, (2) research objectives, and (3) research approach and theoretical background. As a result, a critical analysis of the approaches is presented.

3.1 The aims of the analysis

While scholars and practitioners have put forward 59 IS security awareness approaches, there is a lack of a comprehensive review of the literature exploring these approaches. Such review would be useful for practitioners as they do not necessarily have enough time to browse the large amount of published material. By analyzing the existing IS security awareness approaches, this chapter aims to help practitioners choose IS security awareness approaches that are suitable for the aims and culture of their organization. The results of this analysis are also of value to the research community by creating awareness of alternative IS security awareness approaches and by pointing out what areas of IS security awareness have been studied, and where the need for future research is of greatest importance.

The analysis employs conceptual analysis by reference to Järvinen (1997, 2000) in order to achieve its goals. The first aim is to point out existing IS security awareness approaches that propose concrete means to improve users' security behavior. This is useful for both practitioners and scholars wishing to explore the various approaches further. Furthermore, recognizing a variety of approaches is useful for implementing a combination of several IS security awareness approaches. A combination of approaches is expected to be more efficient than just one approach. For example, exemplary behavior of management together with teaching IS security instructions to end-users can be expected to be more efficient than merely training alone. If managers themselves do not follow IS security instructions, it is not likely that such instructions will be regarded as important by the employees. It is evident, therefore, that teaching them to end-users will not have the desired impact.

In addition to recognizing various IS security awareness approaches, a deeper understanding of these approaches is of value. Lack of understanding of the available IS

security awareness approaches is manifest, for example, in the use of approaches unsupported by adequate empirical evidence on their practical effectiveness. In addition, lack of understanding can become apparent in the use of proposals that do not fit into the culture of the organization in question.

The second aim of this analysis, therefore, is to shed light on the organizational role of IS security evinced by the existing IS security awareness approaches. This can help practitioners to select suitable approaches while avoiding those unsuited to the culture of their organization. For example, proposals which consider people only as means to ensure security may not suit to organization culture where user autonomy is highly valued.

The third goal of the analysis is to contribute to understanding of the theoretical background behind the awareness proposals. This is useful for both scholars and practitioners as understanding the theoretical background increases their knowledge of why a particular IS security awareness approach has (or is expected to have) the intended impact on users' security behavior. In addition, a need to use appropriate theories in the IS discipline has been noted by scholars (e.g., Walls *et al*. 1992).

Furthermore, the fourth aim of the analysis is to draw attention to IS security awareness approaches where empirical evidence has been obtained on their practical efficiency. Achieving this aim is useful for practitioners as such approaches can be considered more credible than approaches that have not been empirically validated.

3.2 Framework for analyzing IS security awareness approaches

In this section, a framework for analyzing IS security awareness approaches is presented. The framework is outlined in Table 3.

The organizational role of IS security

There are three possible perspectives on the role of IS security: *(1) technical, (2) socio-technical, and (3) social* (Iivari & Kerola 1983, Iivari & Hirschheim 1996). It is important to understand how each of the IS security awareness approaches understands the organizational role of IS security and what the attitude toward end users is. This helps practitioners in considering whether the viewpoint of a specific proposal is suitable for their organization's aims and culture.

An IS security approach is considered to be *technical* when its priority is on technical measures and/or technical measures are considered as useful for IS security. In addition, regarding poor technical quality of IS security measures and human resistance as the main causes of IS security problems can be considered as technical standpoint (cf., Iivari & Hirschheim 1996 p. 554-556). Moreover, arguing that IS system users (e.g., employees) must be forced to comply with the IS security policies and instructions represents a technical perspective on IS security. In its ultimate form this may mean considering users bereft of autonomy and advocating the use of punishment in order to achieve their compliance with IS security policies and instructions. In the same vein, emphasizing the surveillance of the users represents the taking of a technical perspective. However, manipulating users towards compliance with IS security policies and

instructions (e.g., through persuasive communication) is a natural goal of any IS security awareness approach and as such is not regarded as seeing IS security from a technical viewpoint.

The *social* view of IS security is end-user-centric, concentrating on social and organizational matters in IS security. Hence, the priority is on issues such as users perceptions and motivational factors regarding compliance with IS security policies and instructions. In addition, considering IS security as a collective, user-related issue as well as addressing organizational issues related to IS security (e.g., feasible IS security processes and procedures) represent the taking of a social standpoint (cf., Iivari & Hirschheim 1996 p. 554-556). Additionally, aspiring that users see IS security as feasible and desirable goal (cf., Iivari & Hirschheim 1996 p. 554-556) is a social viewpoint. Also emphasizing that IS security should impact as little as possible on users' work and/or underlining users autonomy and free will in compliance with IS security policies and instructions come into the category of viewing IS security as having a social organizational role.

The *socio-technical* perspective on IS security is based on interdependent sub-systems, the technical sub-system and the social sub-system, and both systems are considered equally important (Iivari & Hirschheim 1996). In addition, an IS security awareness approach is seen as socio-technical if it lies in between the technical view and social view by giving considerations to both the technical and social aspects of IS security. Furthermore, a socio-technical approach sees lack of fit between the social and technical sub-systems as an important reason for IS security problems (cf., Iivari & Hirschheim 1996 p. 554-556).

Research objectives

Analysis of the existing IS security awareness approaches in the light of their research objectives is useful in highlighting the possible goals of the research. According to Chua (1986) and Habermas (1984), the potential research objectives are *means-end oriented, interpretive or critical*.

Means-end oriented research aims at providing the means to achieve concrete goals or ends (Chua 1986, Iivari 1991 p. 258). In addition, it aims to increase people's control over phenomena (Habermas 1984). Consequently, an IS security awareness approach is regarded as having means-end oriented research objectives when it aims to provide concrete means of modifying users' attitudes toward IS security and their IS security behavior. In addition, a study is considered to have means-end research objectives when it provides concrete means of evaluating the level of IS security and, particularly, users' IS security awareness.

Chua (1986 p. 615) argues that an interpretive scientist aims to enrich people's understanding of the meanings of their actions, thus increasing the possibility of mutual communication and influence. Following this viewpoint, an IS security awareness study is considered to entail *interpretive* research objectives when it aims to contribute to understanding of IS security and, in particular, IS security awareness, and explain it as a phenomenon. In addition, a study that aims to identify the characteristics of IS security awareness and what may influence users' security behavior, is seen to have interpretive research objectives.

Critical research aims at identifying the weaknesses of existing theories and practices – particularly dominant ones. Furthermore, both ideological practice and goals can be subjected to critical analysis (Iivari 1991 p. 258). Consequently, a study that gives critical reconsiderations to the existing IS security awareness approaches is considered to have *critical* research objectives.

Research approach and theoretical background

As stated earlier, it is useful for practitioners to point out IS security awareness approaches that supply empirical evidence for their practical efficiency as such approaches can be considered more credible than approaches lacking such evidence. In addition, acknowledging the theoretical background of existing IS security awareness approaches increases both practitioners' and scholars' understanding of the reasons why a particular approach has the intended impact on employees' IS security behavior.
For this reason, the *research approaches* employed are first analyzed in order to find out what research orientations are used in developing and validating the IS security awareness approaches. With this purpose in mind, the classification of research approaches suggested by Järvinen (1997, 2000) is utilized (see Figure 1).

He divides the approaches to IS research into those using mathematical and those using reality-investigative methods. Further, the approaches to study reality are subdivided into those underlining what reality is and those which stress the utility of artifacts. The approaches stressing what reality is are further divided into conceptual analytical approaches and empirical approaches. The latter are sub-divided into theory-testing and theory-creating approaches. Those approaches which stress the utility of artifacts are divided in turn into artifact-building and artifact-evaluating approaches.

In addition to the research approaches employed, the *theories* underlining the existing IS security approaches are also explored. This is undertaken in order to point out on which theories the existing awareness approaches are grounded on. However, a study is considered to be grounded on a particular theory only if it is explicitly incorporates utilizing this theory.

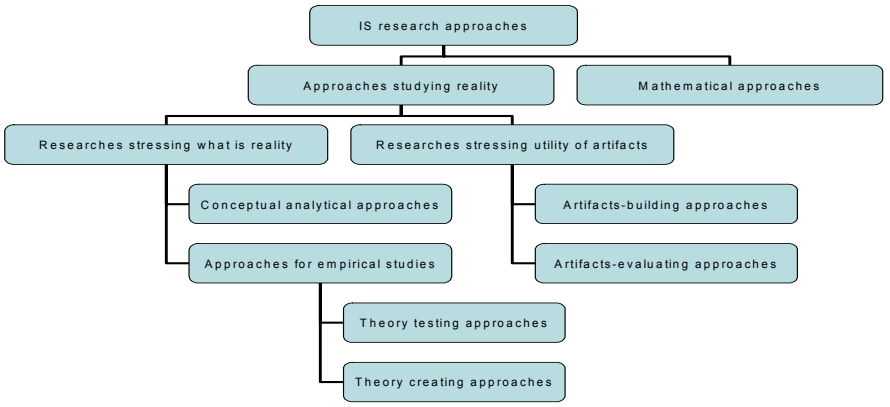

Fig. 1. Järvinen's classification of research approaches (Järvinen 2000 p. 125).

Table 3. An analytical framework for IS security awareness approaches.

Analytical Framework	Aims
Organizational role of IS security	To find out whether the role of IS security is technical, socio-technical or social
Research objectives	To find out whether the objectives are means-end oriented, interpretive or critical
Research approach and theoretical background	To find out which research approaches are used for developing and validating IS security awareness approaches and what their theoretical underpinnings are

3.3 Analysis of existing IS security awareness approaches

In this section, an analysis of the existing awareness approaches is presented. The analysis uses the framework presented in the previous section (see Table 3).

3.3.1 Organizational role of IS security

According to Aytes and Connolly (2003), users' IS security behavior is a result of their own choices, and they argue that a user's behavioral choice is affected by his knowledge about the potential consequences to himself and others. Furthermore, Aytes and Connolly

(2003) claim that an individual's IS security behavior is affected by his estimate of the personal and organizational costs of secure behavior (Aytes & Connolly 2003 p. 2028-2029). As end-user-centric the aforementioned considerations represent the attribution of a social role to IS security.

Banerjee *et al.* (1998) propose that individual characteristics, judgments and beliefs, but also organizational issues (e.g., organizational ethical climate) have an impact on IS employees ethical behavior intentions. Such end-user-centric considerations are evidence of a social view.

Barman (2002) argues that in order to ensure security, all employees with access to an organization's computers and networks should attend mandatory IS security training. Barman also presents an instance in which employees were left without pay until they attended compulsory training sessions or watched them on a videotape (Barman 2002 p. 37). He claims that this is a good way to achieve 100-percent compliance. These views show, proposing enforcement of IS security policies through the aid of mandatory training and punishment, a technical orientation.

Beatson (1991) argues that IS security needs the co-operation of the whole staff. Hence, he considers IS security a collective personnel issue. This represents a social standpoint. However, he also argues that IS security policies developed by management should be enforced and employees should be subject to surveillance and psychological profiling. According to him, this enables employees' dissatisfaction to be predicted before it becomes a security problem. Such considerations, which lead to loss of employee autonomy represent a technical perspective. Beatson (1991) therefore has both social and technical views of IS security, making his view socio-technical in character.

Bray (2002) sees IS security as having a socio-technical organizational role. This is apparent in his statement that security represents a combination of technology (e.g., properly configured firewalls), people and processes all working in balance (Bray 2002 p. 11).

Cox *et al.* (2001) claim that security makes requirements of both technology and users (Cox *et al*. 2001 p.12). According to the Cox *et al.*, secure information systems require good technical solutions, but human behavior is equally important (Cox *et al*. 2001 p. 16). Therefore, users must understand IS security issues and organizations must help their employees to understand IS security issues (*Cox et al.* 2001 p.10-11). The aforementioned considerations with respect to technical and social matters express a socio-technical perspective.

Denning (1999) sees IS as having security a socio-technical role. She balances view between technical and human issues in relation to IS security. The issues addressed by Denning (1999) include, for instance, people's motivation, and societal and cultural aspects. This suggests a social view of IS security. In addition, Denning (1999) considers technique and technology important in ensuring IS security. This indicates a technical standpoint.

Desman (2002 p. xvi) claims that IS security is not a technical issue, but rather a human issue. However, he also emphasizes that technical countermeasures like encryption, alarms, and fire and water detection must be in place. On the basis of his organizational and human-related, but also technical considerations respecting IS security, Desman (2002) adopts a socio-technical perspective.

Forcht *et al.* (1988) emphasize the role of employees, their attitudes, actions and sense of right and wrong in addressing IS security issues. These end-user-centric considerations, in addition to regarding people as independently capable (from their own standpoints) to develop attitudes and a sense of right and wrong, indicate a social perspective on the role of IS security.

Furnell *et al.* (2001, 2002) see IS security as having a socio-technical role. They claim that a comprehensive security solution will encompass physical, procedural, and logical forms of protection (Furnell *et al*. 2002 p. 352, 2001 p. 1), emphasizing the importance of technical and organizational sub-systems which work in mutual balance.

Furnell *et al.* (1997) consider IS security as a personnel issue by stating that it can only be maintained if all employees with access to IS systems know, understand, and accept the necessary precautions. Considering IS security as a staff-related matter is also to take a social view. However, they also claim that staff should receive instructions in how to perform their duties and what is expected from them in terms of IS security by giving them well-defined bounds. Such considerations are evidence of a technical standpoint as users are seen, at least partly, as bereft of autonomy (i.e., their actions should be bounded by rules). In addition, Furnell *et al.* (1997 p. 708) argue for punishment to enforce IS security procedures. This also indicates a social perspective on the role of IS security. On basis of the aforementioned social and technical considerations of IS security, Furnell *et al.* (1997) see IS security as having a socio-technical organizational role.

Gaunt (1998) views IS security as having a socio-technical role. He argues that a successful IS security policy needs to focus on human factors (Gaunt 1998 p. 132) and that implementing the policy requires that the attitudes and educational needs of the employees are taken into account. Seeing IS security as an employee-related matter is to take a social view of IS security. However, he also states that compliance with the policy must be required and enforced by contractual obligation and compulsory training. According to Gaunt (1998 p. 134), access to IS systems should be granted only after signing a confidentiality agreement and attending training. Enforcing IS security policies by denying access to information systems necessary for ones work resembles punishment and as such, means that employees' autonomy is restricted. This is a technical standpoint.

Gaunt (2000) also sees IS security as a socio-technical issue. His technical viewpoint becomes evident by claiming that the employees' behavior must be changed in order to get them to comply with IS security policies (Gaunt 2000 p. 152). He also argues that reluctance to change is widespread among users. According to Iivari and Hirschheim (1996 p. 555), taking human resistance as a reason for implementation problems represents a technical viewpoint. Furthermore, Gaunt (2000 p. 153) considers poor technical quality of IS security controls as another impediment to change. This, too, is to take a technical standpoint (cf., Iivari & Hirschheim 1996 p. 555). However, Gaunt (2000 p. 153) also deals with organizational matters – such as inconsistent IS security policies between organizations and conflicting demands between the need to openness and to maintaining confidentiality of information – as a hindrance to compliance with IS security policies. This is to adopt a social standpoint.

Hadland (1998) represents a socio-technical frame of reference in claiming that both the technical and social aspects of IS security are important (Hadland 1998 p. 93). However, he argues that successful IS security management relies even more heavily on

a high level of end-user cooperation than on technical matters (Hadland 1998 p. 93-94). His socio-technical viewpoint is therefore closer to a social perspective than a technical one.

Hansche (2001a p. 15-16) maintains that employees are one of the most important factors in ensuring IS security. According to her, most employees are not aware of the consequences of their actions, causing many IS security incidents. She also claims that IS security is seen as a hindrance by most IS users. Iivari and Hirschheim (1996 p. 555) argue that a technical viewpoint on IS issues emphasizes human resistance as a major source of implementation problems. Hansche (2001a) thus sees IS security as having a technical role. However, Hansche (2001a p. 15-16) also claims that users who are aware of IS security issues are also the single most important asset in detecting and preventing IS security incidents. Seeing an employee as an asset (rather than an instrument) to ensure security is to take a social view of IS security. Consequently, Hansche (2001a) presents a socio-technical frame of reference. Hansche (2001b) continues the work of Hansche (2001a) and shares the same view of IS security. Consequently, Hansche (2001b) takes a socio-technical view of the organizational role of IS security.

ISF (2005) sees IS security from a socio-technical viewpoint. This is evident in the standard's balanced view of organizational aspects of IS security (e.g., business requirements of security, arranging IS security management and IS security organization, setting up an organizational security classification scheme), technical aspects of IS security (e.g., use of cryptography, application security, computer installation security, network security) and human aspects of IS security (e.g., important role of employees in IS security).

ISO (2005) gives balanced considerations on organizational, technical and human aspects of IS security, which indicate a socio-technical viewpoint. Furthermore, the standard claims that new employees should attend IS security awareness training before access to information or services is granted. According to this recommendation, an employee may be left without access to information systems and information necessary for completing his work. This resembles the use of punishment and as such, is evidence of a technical view. In addition, the standard argues for disciplinary actions is case of violations against IS security policies, which is also to take a technical standpoint.

Kabay (2002 p. 35.2) argues that security depends on people more than on technology. The study addresses IS users' group behavior including social arousal, locus of control, group polarization and group thinking. These considerations regarding the individual's behavior in social groups demonstrates a social perspective. However, Kabay (2002) argues for sanctions in order to achieve compliance (Kabay 2002 p. 35.13), thereby also taking technical view of IS security. Thus, the organizational role of IS security presented by Kabay (2002) is a socio-technical one.

Kajava and Siponen (1997 p. 111) argue that IS security guidelines should be planned in a way which enables employees to complete their work with as few extra considerations as possible. In addition, an IS security awareness program should meet the social requirements stipulated by the culture on the organization (Kajava & Siponen 1997 p. 113). According to Kajava and Siponen (1997), understanding and respecting human factors is the only way to gain the acceptance of employees (Kajava & Siponen 1997 p. 113). The aforementioned human-centric considerations represent a social standpoint.

On the basis of his human related viewpoint, Katsikas (2000) has a social perspective on IS security. The study deals with an IS security awareness that aims at bettering managers' understanding of IS security helping them to cope with management tasks related to IS security (Katsikas 2000 p. 134). He also emphasizes that individual needs must be assessed when IS security training is developed and delivered.

Kluge (1998) addresses issues related to ethical guidelines for a health care professional (HIP). These guidelines govern a HIP in protecting electronic patient information. Such constraints result from the relationship between patients and the HIP, but also from the needs of the institution, society and healthcare as a profession. For these reasons, the study sees IS security as having a social organizational role.

Kovacich (1998) argues that the full support and cooperation of users are necessary in establishing and maintaining a successful organizational IS security program. He addresses user-related issues, but also technical issues as these are related to IS security. Kovacich (1998) therefore takes a socio-technical perspective on IS security.

Kovacich and Halibozek (2003) emphasize the human aspect in ensuring security. This is to take a social viewpoint. They also argue for security awareness training program that aims to make users comply with security policies (Kovacich & Halibozek 2003 p. 258) and claim that human resistance is the main obstacle to effective training. This represents a technical view of IS security (cf., Iivari and Hirschheim 1996 p. 555). Consequently, Kovacich and Halibozek (2003) see IS security as having a socio-technical role.

Lafleur (1992) takes a socio-technical perspective on the organizational role of IS security. He argues that IS security depends on both organizational and technical systems (Lafleur 1992 p. 4). Threats to IS security can be caused by failures in either the technical or organizational systems (Lafleur 1992 p. 4). Such considerations of two separate sub-systems that should work in balance are evidence of a socio-technical viewpoint.

Markey (1989) sees IS security as having a socio-technical role. She argues that the effectiveness of a systems security program depends on the security of automated systems and physical security (Markey 1989 p. 83, 86). These issues show a technical standpoint. However, she also claims that security policy objectives and security procedures must have the support of the whole organization. Furthermore, the policies and procedures should be constructed to support the mission of the organization, which requires that all concerned parties must have an opportunity to review and accept them (Markey 1989 p. 85). Such organizational considerations indicate a social viewpoint.

Martins and Eloff (2002) opine that the effectiveness of IS security depends on technical measures as well as on the people implementing and using them (Martins & Eloff 2002 p. 203-204). This viewpoint is socio-technical in nature through the attention paid equally to technical and human-related issues. Moreover, the socio-technical role of IS security becomes apparent in the combination of social considerations addressing organizational, group, and individual level security issues (Martins & Eloff 2002 p. 206-210) and the technical considerations when the study argues for controlling users behavior (Martins & Eloff 2002 p. 210).

McLean (1992 p. 179) argues that changing employees' values, perceptions and behavior is necessary in order to achieve a satisfactory level of IS security. The study explores factors affecting human behavior and attitudes and how change in them can be enforced through the aid of a security awareness campaign. Such considerations, by both

emphasizing the human aspect of IS security but also regarding employees' to some extent as bereft of autonomy shows IS security to have a socio-technical role.

Mitnick (2002) takes a socio-technical view of IS security. The view is social in that security is not seen as a problem of technology, but rather a management and people-related problem (Mitnick 2002 p. 4). According to him, there is no technology that can prevent a social engineering attack (Mitnick 2002 p. 245). However, he also engages in technical considerations by arguing for punishment in order to change the behavior and attitudes of users (Mitnick 2002 p. 249).

Murray (1991) states that companies often implement good technical IS security measures (e.g., power supply backup), but forget to make their staff aware of those measures and provide them with IS security instructions to follow. Consequently, most IS security problems are caused by employees who do not appreciate the risks inherent in their actions. Murray (1991), thus, sees a misfit between the technical and social/organizational sub-systems as the primary hindrance for implementing good IS security. This represents a socio-technical viewpoint.

NIST (1996 p. 145) has a balanced view of the technical, organizational, and human factors relevant to ensuring good IS security. In addition to technical and organizational IS security measures, NIST (1996) considers also end-users a critical factor in guaranteeing the security of computer systems. This represents a socio-technical viewpoint.

NIST (1998) describes a methodology for setting up an IS security awareness training program that is based on each employee's specific role in the organization. Consequently, it takes a social view of IS security by giving consideration purely to organizational issues.

Similarly, NIST (2003) deals purely with organizational issues related to setting up IS security awareness training. By this token, the document takes a social perspective on IS security.

Parker (1998) discusses both technical issues, but also issues related to motivating end-users on behalf of IS security and building security on the performance of people. This includes using rewards, peer-pressure and removing conflicts between job performance and security constraints in order to ensure secure behavior. Such considerations as these related to end-users together with considerations regarding technical aspects of IS security are evidence of a socio-technical standpoint. Moreover, the technical viewpoint becomes apparent in his argument that violation of security guidelines and instructions is unwanted behavior that needs to be controlled through the aid of punishment. To conclude, Parker (1998) sees IS security having a socio-technical role. In the same vein, Parker (1999) engages in a socio-technical viewpoint. The main points regarding the role of IS security are the same as in Parker (1998). In addition, the study takes the view that security is equally dependent on both social and technical systems (Parker 1999 p. 15).

Peltier (2000, 2002) maintains that employees are a critical factor in ensuring IS security. Consequently, they need to understand why IS security must be taken seriously, what they will gain from its implementation, and how it will help them in completing their tasks (Peltier 2000 p. 23, 2002 p. 149). In addition, he claims that IS security represents a cultural change (Peltier 2000 p. 29, 2002 p. 159). These considerations of organizational and user-related matters represent a social viewpoint. However according

to Peltier (2000 p. 29, 2002 p. 159), once employees are conscious of a security program, they are obligated to comply with it. Such a view is technical by reference to the fact that people are considered to some extent as bereft of autonomy. Therefore, the studies by Peltier (2000, 2002) reflect a socio-technical perspective.

Perry (1985 p. 8) argues that IS security is a people-related problem and that the solution to computer security is through people. Moreover, he presents various means to create the kind of supportive organizational environment necessary in order to change people's behavior (Perry 1985 p. 93-94). Thus, Perry recognizes the human and organizational aspects of IS security. However, Perry also assesses the technical issues related to security. This represents a technical perspective. The combination of human-related and technical considerations indicates that the viewpoint presented by Perry (1985) is socio-technical.

Pipkin (2000 p. 101) states that IS security awareness is a process that aims at user understanding of the implications of IS security, the use of IS security measures, and how IS security violations are reported (Pipkin 2000 p. 101). Thus, Pipkin (2000) deals with the end-user-centric aspects IS security, which is evidence of a social viewpoint. However, he also suggests that violations against IS security policies represent inappropriate behavior that must be changed by using punishment. This in turn represents a technical viewpoint. Thus, Pipkin (2000) takes a socio-technical perspective on the organizational role of IS security.

Proctor and Byrnes (2002 p. 21) argue that the implementation of security must address technology, processes and procedures. They consequently present a socio-technical view of IS security by presenting a balanced view of technical and social systems.

Similarly, Rudolph *et al.* (2002) see IS security as having a socio-technical role. They consider IS security as a people-related issue (Rudolph *et al.* 2002 p. 29.4). This indicates a social viewpoint. In addition, they consider failure to comply with IS security policies as improper behavior that must be changed through the aid of penalties (Rudolph *et al*. 2002 p. 29.2). This in turn displays a technical viewpoint.

Sasse *et al*. (2001) present a socio-technical perspective on IS security. Their main design approach to security is human/computer interaction (HCI), and they claim that security is a socio-technical system (Sasse *et al*. 2001 p. 130). HCI takes into account the fact that users and technology work together in achieving a goal. Achieving the goal requires that the design of the social and technical systems is balanced. This represents a socio-technical viewpoint.

According to Schlienger and Teufel (2002 p. 195), IS security management requires *"a socio-cultural, human centric approach based on trust and partnership, accompanied by appropriate security technology."* They emphasize the importance of an IS security culture that focuses on the socio-cultural aspects of IS security management. In addition to the cultural aspects of IS security, they consider technology to have an important role. They therefore present, for the most part, a social perspective on IS security, but technical considerations are also taken into account. Hence, their viewpoint is a socio-technical one.

Siponen (2000a) addresses end user-related and organizational IS security matters. He lays stress on human nature in enhancing IS security and underlines the necessity of employees' commitment to IS security. Furthermore, he addresses issues related to an

individual's motivation and attitude (Siponen 2000a p. 33-34) and presents a persuasion framework to be used in security education (Siponen 2000a p. 37-38). The study thereby recognizes the human component in IS security and thus has a social perspective. However, Siponen (2000a) also proposes punishment in order to achieve users compliance with IS security policies, thus also bringing a technical approach to bear on IS security.

Siponen (2000c) presents a social perspective on IS security. He explains the need for human morality in enhancing IS security within organizations. In addition to human-related issues, Siponen (2000c) addresses organizational matters, including the need for morality in business, removing double standards of morality, displaying moral respect for employees, and facilitating an open climate for communication. Such human-oriented and organizational considerations represent a social viewpoint. Siponen (2000c) also emphasizes users' free will and autonomy, which further represents a social viewpoint.

Spurling (1995) presents IS security as having a social role. He argues that building commitment to IS security on the part of users involves providing a process that fits in with the organizational culture (Spurling 1995 p. 20). In addition, he states that it is vital to gain the support of the whole organization (Spurling 1995 p. 21) Additionally, Spurling (1995 p. 23) presents a security philosophy that aims to "*open up access as far as it is possible within the constraints of good business practice*." He states that the above philosophy has allowed his company to dispense with unnecessary chasing after violations (Spurling 1995 p. 23). Furthermore, Spurling addresses means helping users cope with their work giving as little considerations to security as possible. Finally, Spurling (1995 p. 24) argues that the most important factor in good IS security is to listen to and understand users' security concerns. All the aforementioned issues indicate a social standpoint.

Stacey (1996) addresses issues related to an organization's maturity from the perspective of IS security. By considering IS security mainly as an organizational issue, the study takes a social viewpoint.

Straub (1990) presents a technical perspective on IS security. The study argues for sanctions to be used in cases of violations of IS security guidelines and the effect of such sanctions on deterring others from violating the guidelines. Seeing violation of security guidelines as unwanted behavior that must be controlled through the aid of punishment indicates a technical viewpoint. In the same vein, Straub *et al*. (1993) express a technical viewpoint by arguing for punishment in order to achieve user compliance with IS security policies. Also Straub and Welke (1998) argue on behalf of deterrence, thereby presenting a technical viewpoint.

SSE-CMM (1999) takes a socio-technical view of IS security. The document deals with organizational processes as related to security engineering activities. In addition, it addresses issues related to system users' IS security awareness. These issues reflect a social viewpoint. However, SSE-CMM also deals with technical issues like the secure configuration of devices. Consequently, SSC-CMM presents IS security as a socio-technical issue.

Telders (1991) sees IS security as socio-technical. The study describes technical development as having created an increased need to improve users' IS security awareness. Emphasizing the importance of technology represents a technical standpoint. In addition, Telders (1991) claims that the primary problem with IS security is lack of

users' motivation. This, too, represents a technical viewpoint. However, Telders' (1991) social standpoint becomes evident in his considerations of user awareness and feasible processes and procedures as necessary for good IS security.

GASSP (I^2SF 1999) presents a socio-technical perspective on IS security. The document defines system as *"an umbrella term for the hardware, software, physical, administrative, and organizational issues that need to be considered when addressing the security of an organization's information resources"* (I^2SF 1999 p. 13). Thus, social and technical sub-systems are considered to be equally important. This represents a socio-technical viewpoint.

Thomson and von Solms (1997 p. 96) argue that technology cannot cover a management lapse, but sound management practices can cover technical shortcomings. Considering such organizational issues as important represents a social viewpoint. In addition, the study addresses such organizational issues of IS security as the purpose of organizational IS security policies. However, technical issues like the growth of networking and linking to the Internet are also considered as relevant for IS security. On basis of the social and technical considerations, Thomson and von Solms (1997) present a socio-technical view of IS security.

Thomson and von Solms (1998) also present a socio-technical view of IS security. The study discusses various technical issues which have had an impact on IS security and created the requirements for users awareness. Such considerations represent a technical standpoint. However, the study also argues that it is not possible to maintain effective IS security with physical and technical controls alone: human matters must also be considered. For this reason, the study discusses human behavior and IS security awareness from a social-psychological viewpoint. As it is end-user centric, the latter viewpoint is a social one.

Tudor (2001) presents a socio-technical perspective on IS security. She underlines the necessity for users' IS security awareness and discusses how to motivate users with respect to IS security. This is a social standpoint. However, Tudor argues for deterrence as a means to achieve security-positive behavioral changes on the part of users, which represents a technical viewpoint. Tudor also addresses various aspects of security technology (e.g., encryption, public key infrastructure, firewalls, virtual private networks, smartcards, remote access servers, and biometrics) (Tudor 2001 p. 201-237). Addressing such technical issues signifies a technical viewpoint.

The organizational role of IS security presented by Vroom and von Solms (2002) is socio-technical in character. They state that security is dependent equally on technical, physical, and operational controls as well as on user behavior (Vroom & von Solms p. 21). In addition, they consider the technical and organizational issues of IS security as equal.

Vyskoc and Fibikova (2001) present a socio-technical view of IS security. They aim to find out how users perceive IS security. In addition, they consider IS security as a people-related problem (Vyskoc & Fibikova 2001 p. 1). The study thereby underlines the importance of the human aspects of IS security. This is a social viewpoint. However, the study also takes a technical perspective in arguing that users' improper security behavior must be changed as it is a major reason for inefficient security measures.

White House (2003a, 2003b) presents a social view of IS security. The studies address societal and organizational issues of IS security concerning private sectors, organizations, individuals and the United States as a whole.

In Wood (2002), the organizational role of IS security is socio-technical. He argues that IS security is simultaneously a people-related issue, a technology issue and a management issue. However, the study gives consideration mainly to human, organizational and societal issues. Thus, the viewpoint is closer to a social than a technical one.

Wood (1995) takes a socio-technical perspective on IS security. His technical viewpoint is apparent in his considerations of users' failures to comply with security instructions as improper behavior that should be punished (Wood 1995 p. 14). However, considerations of various organizational issues such as organizational structures, change approval and test processes, and an organizational problem reporting system, are also provided. Such organizational considerations represent a social viewpoint. In addition, the social standpoint is visible when Wood (1995) argues that the support of end-users is necessary for implementing successful security measures.

3.3.2 Research objectives

Aytes and Connolly (2003) aim at improving the understanding of behavior-related aspects of IS security (Aytes & Connolly 2003 p. 2028). The study presents a model of user behavior that *"emphasizes the factors relating to the user's perception of risks and the choice based on that perception"* (Aytes & Connolly 2003 p. 2027). Thus, Aytes and Connolly (2003) have interpretive research objectives.

Banerjee *et al.* (1998) seek to "identify characteristics that are associated with and may influence the ethical behavior intention of information systems employees when faced with ethical dilemmas" (Banerjee et al. 1998 p. 31). Therefore, the study has interpretive research objectives.

Barman (2002) offers means to write and implement security policies by explaining how to start a policy writing process as well as how to write and maintain such policies. By this token, the study has means-end research objectives.

Beatson (1991) also has means-end research objectives by proposing means to maintain a high level of IS security awareness in order to avoid security breaches.

Bray (2002) has means-end research objectives offering concrete means that can be used to improve users' IS security awareness in order to avoid security breaches during reductions in the workforce.

Similarly, Cox *et al*. (2001) suggest concrete means to reach a high level of awareness specific to users' IS security (Cox *et al*. 2001 p. 11). The study therefore has means-end oriented research objectives.

The research objectives of Denning (1999) are interpretive. She aims at adding to the understanding of readers with respect to information warfare by describing and explaining it as a particular phenomenon (Denning 1999 p. xii-xiv). As one of the major points of vulnerability is people (Denning 1999 p. 382), the study aims to contribute to understanding of the role of IS security awareness in defensive IS security warfare.

Desman (2002) has an approach which is means-end in its orientation. The study presents means for creating an IS security awareness program (Desman 2002 p. x).

The study by Forcht *et al*. (1988) has interpretive research objectives. The study aims at increasing understanding in the area of computer ethics by exploring ethical problems raised in the computer environment.

Furnell *et al*. (2001, 2002) have objectives which are oriented towards means-end research. The goal is to provide concrete means to achieve better IS security by describing the implementation of a software tool. This tool is meant for self-paced security training.

Furnell *et al*. (1997) present factors that health care establishments should consider in setting up a training and awareness framework. However, the study does not provide the concrete means for setting the framework. Rather, it attempts to increase understanding with respect to issues worth considering. The study consequently has interpretive research objectives.

Gaunt (1998) has objectives which are both means-end and interpretive in their orientation. He recounts the experience of an IS security project in a hospital and with the aim of increasing understanding of the obstacles that any organization may face during such a project (Gaunt 1998 p. 131). This is an interpretive objective. In addition, the study offers concrete means to overcome such obstacles. This shows a means-end objective.

For similar reasons to Gaunt (1998), Gaunt (2000) also has objectives which are both interpretive and means-end in their orientation.

Hadland (1998) describes concrete means used in an example organization to raise users' IS security awareness. His research objectives therefore are, in their orientation, means-end.

Hansche (2001a) also offers advice on creating an IS security awareness program (Hansche 2001a p. 14). Therefore, this study also has objectives which are oriented to means-end research. In addition, Hansche (2001b) entertains means-end research objectives by suggesting means to develop an IS security-training program.

ISF (2005) has objectives which are oriented towards means-end research in providing means to build a practical, business-oriented basis for assessing an organization's IS security arrangements.

ISO (2000) makes recommendations to security professionals on how to initiate, implement and maintain security. The purpose of these recommendations is to provide means to enhance IS security, and as such, they represent research objectives which are means-end in their orientation.

Kabay (2002) has objectives which are oriented to both means-end and interpretive research. First, the study aims to increase understanding of how best to work with human predilections and predispositions (Kabay 2002 p. 35.2). This is an interpretive objective. Second, the study argues that such understanding provides the means to improve security and implement security policies effectively (Kabay 2002 p. 35.2). This indicates a means-end oriented research objective.

Kajava and Siponen have research objectives which are means-end in their orientation. They present tools and methods for increasing IS security awareness in organizations, within the context of a Finnish university.

Katsikas (2000) has objectives oriented to means-end research by reference to his aim of presenting a methodology for determining the training needs of employees (Katsikas 2000 p. 129).

Also Kluge (1998) has objectives which are oriented to means-end research. The study offers means to protect electronic patient records by presenting a model code of ethics for health information professionals.

Kovacich (1998) has objectives oriented to means-end research given his stated goal of presenting means to achieve users' support for an IS security program.

In the same vein, Kovacich and Halibozek (2003) have means-end oriented objectives. They present methods aimed at increasing users´ awareness and understanding of IS security, and motivating them to protect corporate assets.

Lafleur (1992) has objectives which are oriented to both interpretive and means-end research. He seeks to explain the human characteristic of resistance to change (Lafleur 1992 p. 4-5) and to increase the reader's understanding of users' behavior. This is an interpretive research objective. In addition, the goal of the study is to find the means to overcome user resistance, which is a means-end objective.

The study by Markey (1989) shows means-end oriented research objectives by proposing means to increase awareness on the part of organizations and encourage their involvement in computer security.

The first aim of Martins and Eloff (2002) is to present a model of security culture. The purpose of the model is to increase the understanding of IS security. It therefore indicates an interpretive research objective. In addition, they present a concrete assessment approach that is meant as a tool to evaluate an organizational security culture. This represents a means-end oriented objective. The study thereby has both interpretive and means-end research objectives.

McLean (1992) also has interpretive and means-end oriented research objectives. First, the study aims at explaining the behavior of users (McLean 1992 p. 180-184), which is an interpretive objective. However, the study also presents a concrete plan for an IT security awareness campaign (McLean 1992, p. 190-192). The campaign aims at changing user behavior and thus represents an objective oriented towards means-end research.

Mitnick (2002) has interpretive and means-end research objectives. His efforts to explain human manipulation (Mitnick 2002 p. 246-249) indicate an interpretive research objective. He also presents a structure to and the contents of security awareness training. This is an objective oriented towards means-end.

Murray (1991) has interpretive research objectives. He wishes to increase understanding of the potential problems associated with poor IS security. In addition, he puts figures on the size of the problem in the United Kingdom.

NIST (1996) has objectives which are oriented towards both interpretive and means-end research. The interpretive objectives are apparent in the efforts to increase understanding of the differences between awareness, training and education. However, the study also presents an approach that can be used to develop a computer security awareness and training program. The framework aims to provide concrete means to increase users' IS security awareness and thus indicates a means-end objective. The same also applies to NIST (1998) and NIST (2003).

The studies by Parker (1998, 1999) have objectives oriented towards both interpretive and means-end research. First, the studies aim at increasing understanding of end users' behavior by explaining motivation-based factors and attempting to motivate through self-interest. This is an interpretive objective. In addition, Parker (1998, 1999) presents concrete means to increase motivation and awareness on the part of the end-user, which represents a means-end research objective.

The studies by Peltier (2000, 2002) have objectives oriented towards means-end research. Peltier's (2002) interest is in providing means of developing and implementing IS security policies, procedures and standards (Peltier 2002 p. xii-xiv). Peltier (2000) in turn provides tools to implement a security awareness program (Peltier 2000 p. 23).

Perry (1985) has objectives which are oriented towards both interpretive and means-end research. The study aims at interpreting the behavior of people and the factors which induce behavioral change, and thus represents an interpretive research objective. In addition, it presents means for the creation of enthusiasm on behalf of computer security through the aid of a favorable environment and individual enthusiasm, thereby having a means-end research objective.

Pipkin (2000) seeks to unveil issues surrounding IS security (Pipkin 2000 p. xix). In addition, the study is meant to be an introduction to IS security (Pipkin 2000 p. xix). He does not present any concrete means to resolve any specific security problem. Rather, the aim is to increase understanding with respect to various issues related to IS security. One of these issues is IS security awareness. Pipkin (2000), therefore, has interpretive research objectives.

Proctor and Byrnes (2002) discuss security from the business perspective. They provide brief considerations of an IS security awareness program as part of a more general IS security program. This discussion aims at increasing understanding of the subject. Concrete means for implementing such a program are not presented. The research objectives of the study may therefore be said to be interpretive.

Rudolph *et al*. (2002) have means-end oriented research objectives in their efforts to provide a program to enhance employees' IS security awareness.

Sasse *et al.* (2001) have interpretive research objectives in their aim of increasing understanding of how human/computer interaction can be employed in security design (Sasse *et al*. 2001 p. 123).

Schlienger and Teufel (2002) have interpretive research objectives. They present the concept of an organizational security culture and explain how cultural theory can be used in understanding the concept.

Siponen (2000a) has objectives oriented towards critical, interpretive and means-end research. He aims to outline a behavioral framework explaining how people can be motivated on behalf of IS security and how they may respond to efforts which seek to increase awareness. He also explains the concept of prescriptive awareness and the need for such awareness. The aforementioned issues increase readers' understanding and as such are interpretive objectives. In addition, the study performs critical reconsiderations of some of the existing methods and approaches for increasing awareness. This signals a critical research objective. Finally, Siponen (2000a) presents a persuasion strategy meant to induce user commitment to security guidelines. This shows an objective which is means-end oriented.

Siponen (2000c) also has critical, interpretive, and means-end oriented research objectives. The critical objectives of the study are seen when Siponen shows that the argument against the relevance of human morality as a means of protection is unreasonable. In addition, he clarifies the theoretical foundations of how human morality can be used as a means of protection, which is an interpretive objective. Finally, he proposes an approach that aims to protect information through the aid of human morality. This indicates an objective which is means-end oriented.

Spurling (1995) presents various means to establish commitment to security on the part of users and management. Thus, his objectives are means-end oriented.

Stacey (1996) offers various means to evaluate an organization's maturity from the perspective of IS security. However, the study reflects objectives which are oriented towards both interpretive and means-end research. The tool is an instrument to achieve a concrete goal: an evaluation of the maturity of an organization by reference to its IS security management. This signifies an objective which is means-end in its orientation. In addition, the use of the tool aims to increase understanding of IS security in a particular organization, which reflects an interpretive objective.

The research objectives of Straub (1990) are oriented towards both means-end and interpretive criteria. He aims to find out to what extent management-derived investments in security result in lower risk from computer abuse (Straub 1990 p. 2). This increases understanding of the use of deterrence and is therefore an interpretive objective. However, the study also aims to provide means to change users' behavior with the aid of deterrence. Thus, Straub (1990) also entertains objectives which are means-end oriented.

The aim of Straub *et al*. (1993) is to find out how student cheating can be deterred (Straub *et al*. 1993 p. ii). Thus, the study has objectives with a means-end orientation.

Straub and Welke (1998) propose various means to raise managers' IS security awareness and enhance an organization's IS security. Thus, the study has means-end oriented research objectives. However, it also has interpretive objectives in its efforts to increase understanding of issues related to IS security management such as the nature of system risks (Straub & Welke p. 442-443), managerial perceptions of security risk (Straub & Welke p. 443-445), and actions for managing systems-related risks (Straub & Welke p. 445-447).

SSE-CMM (1999) "*describes the characteristics of an organization's security engineering project that must exist to ensure good security engineering*" (SSE-CMM 1999 p. 1). The objective of the SSE-CMM is to advance security engineering as a discipline that is defined, mature and measurable. SSE-CMM has been developed to enable focused investment in security engineering tools, capability-based assurance, and a selection of appropriately qualified providers of security engineering (SSE-CMM 1999 p. 2). The document therefore has objectives with a means-end orientation.

Telders (1991) aims to help data security managers develop and implement an IS security awareness program (Telders 1991 p. 57). The study also thereby entertains objectives which are means-end in their orientation. However, Telders (1991) also engages in interpretive objectives by trying to explain the reasons for developing an awareness program.

The goals of GASSP are (I^2SF 1999 p. 3): (1) the international harmonization of culturally neutral IS security, (2) the elimination of artificial barriers to the free flow of information worldwide, (3) the definition and implementation of a principled foundation

for an industry, (4) making provision for the rapidly evolving nature of IS security methods, issues, and technology, and their articulation in principle, and (5) identifying the corresponding management issues. The aims of realizing the aforementioned goals represent an objective with a means-end orientation.

Thomson and von Solms (1997) present an IS security awareness program which is targeted at improving IS security awareness at three organizational levels: top management, information systems management and end-users. They thereby engage in an approach which is means-end oriented. However, the model presented is assumed to be more effective than existing proposals (Thomson & von Solms 1997 p. 93). The study consequently also has critical objectives.

Thomson and von Solms (1998) have objectives which are oriented towards both interpretive and means-end research. They attempt to highlight the reasons why an IS security awareness program should receive attention in all organizations (Thomson & von Solms 1998 p. 167) as well as attempting to increase readers' understanding of a human attitude system and concepts of social psychology (Thomson & von Solms 1998 p. 168-172). This signifies an interpretive objective. In addition, the study aims to show specifically where certain concepts can be used (Thomson and von Solms 1998 p.172), which represents a means-end oriented research objective.

Tudor (2001) has objectives which are oriented towards both interpretive and means-end research. The study aims at increasing readers' understanding of what an IS security awareness program and its objectives are. This is an instance of an interpretive research objective. In addition, Tudor presents means to implement such an awareness program (Tudor 2001 p. 154-159). This represents a means-end oriented objective.

Vroom and von Solms (2002) aim to increase the reader's understanding of IS security issues by explaining the history of IS security. In addition, they seek to explain the reasoning behind an IS security awareness program as well as some of the elements of such a program. Moreover, the study attempts to present a conceptual model of IS security awareness. These aims reflect interpretive research objectives. However, the study also has objectives which are oriented to means-end goals by presenting concrete means for the practical implementation of an IS security awareness program.

Vyskoc and Fibikova (2001) entertain interpretive research objectives in their aims to evaluate what information technology users think about IS security matters and compare that with the expectations of security specialists (Vyskoc & Fibikova 2001 p. 2).

White House (2003a, 2003b) has interpretive research objectives. The two studies attempt to increase understanding of issues related to securing cyberspace. They give consideration to the role and responsibilities of home users, small businesses, large enterprises, institutions of higher education, the private sector, state and local governments.

Wood (2002) outlines various principles relating to the building of better IS security awareness in organizations (Wood 2002 p. 15). However, no concrete means of improving users' IS security behavior are presented. Rather, the study aims to increase the reader's understanding of the human issues related to IS security. The study thereby reflects interpretive research objectives.

Wood (1995) has objectives which are means-end oriented in presenting a list of potential means to increase users' IS security-related awareness.

3.3.3 Research Approach and Theoretical Background

Aytes and Connolly (2003) present a model of human security behavior by employing conceptual analysis. The model is based on the findings of Slovic's study regarding human perception of risk (Slovic, 1987). In addition, the model utilizes the results of the existing research on humans' reactions to risks (e.g., Fischhoff, Slovic, & Lichtenstein 1978, Fischhoff, Slovic, Lichtenstein, Read & Combs 1979, Zeckhauser & Viscusi 1990) and people's general attitude towards risk (e.g., Weber and Milliman 1997).

Banerjee *et al*. (1998) is a theory-testing empirical study. The study presents a framework for exploring ethical behavior (Banerjee *et al.* 1998 p. 32-38). The framework is tested with a survey. The theoretical base of the framework includes the theory of reasoned action (Fishbein & Ajzen 1975), the theory of planned behavior (Ajzen 1991) and Kohlberg's theory of moral development (Kohlberg 1981).

Barman (2002), Beatson (1991), Bray (2002), Cox *et al* (2001), Denning (1999), Desman (2002), Forcht *et al*. (1988), Furnell *et al*. (1997, 2001, 2002), Gaunt (1998, 2000), Hadland (1998), Hansche (2001a, 2001b), ISO (2000), ISF (2005), Kabay (2002), Kajava and Siponen (1997), Kluge (1998), Katsikas (2000), Kovacich (1998), Kovacich and Halibozek (2003), Lafleur (1992) and Markey (1989) all employ conceptual analysis, but do not present the theoretical background to their IS security awareness approaches.

Martins and Eloff (2002) is a theory-testing empirical study. They create a model for security culture and a method of assessment designed to evaluate the IS security culture of an organization. The method is tested in a case study where it is employed to evaluate the IS security culture of an IT consultancy organization. Neither the model nor the assessment approach is accompanied by a theoretical background.

McLean (1992) employs conceptual analysis. Moreover, the study utilizes the stimulus-response model (e.g., Skinner 1991 p. 9) and Rogers' model of the adoption of innovations (Rogers 1962) as its theoretical background.

Mitnick (2002), Murray (1991), NIST (1996), NIST (1998), NIST (2003), Parker (1998, 1999), Peltier (2000, 2002), Perry (1985), Pipkin (2000), Proctor and Byrnes (2002), and Rudolph *et al*. (2002) employ conceptual analysis. However, these studies do not present the theoretical background to their IS security awareness approaches.

Sasse *et al*. (2001) employ four empirical theory-creating studies that create new theoretical information related to reasons for login failures and the poor usability of password mechanisms, but without presenting a theoretical background for their approach.

Schlienger and Teufel (2002) employ conceptual analysis in explaining a model for IS security culture, but without presenting the theoretical background of their study.

Siponen (2000a) employs conceptual analysis and presents a behavioral framework based on the following theories: theory of reasoned action (Fishbein & Ajzen 1975), theory of planned behavior (Ajzen 1991), intrinsic motivation (Deci & Ryan 1985), the principle of the "veil of ignorance" (Rawls 1999), Hare's overriding thesis (cf., Hare 1981), and the technology acceptance model (Davis 1989).

Siponen (2000c) employs conceptual analysis. The underlying theories are Hare's overriding thesis (cf., Hare 1981) and the concept of the veil of ignorance by Rawls (cf., Rawls 1999).

Spurling (1995) and Stacey (1996) employ conceptual analysis, but do not present the theories underpinning their IS security awareness approaches.

Straub (1990), Straub *et al.* (1993), and Straub and Welke (1998) are based on the theory of general deterrence. Straub (1990) investigates whether a management decision to invest in information system security results in more effective control of computer abuse. It is a theory testing study providing empirical evidence for the general deterrence theory. Straub *et al*. (1993) is also a theory-testing study that provides empirical support for the general deterrence theory. It presents the results of a replicated field experiment that explores how student cheating on computer programming assignments can be deterred. In addition, Straub and Welke (1998) is a theory-testing empirical study. It explores whether managers are fully aware of the range of generic security actions which research links to lower system risks (Straub & Welke 1998 p. 447).

SSE-CMM (1999), Telders (1991), I^2SF, Thomson and von Solms (1997, 1998), Vroom and von Solms (2002), and Tudor (2001) employ conceptual analysis, but do not explicitly present any underlining theories.

In addition, Vyskoc and Fibikova (2001) is a theory-creating empirical study. However, the theoretical background of the study is not explicitly presented. Furthermore, Wood (1995, 2002) and White House (2003a, 2003b) employ conceptual analysis, but do not present the theories underlying their IS security awareness approaches.

3.4 Conclusion of the analysis

In this chapter, the existing IS security awareness approaches were explored from the following three viewpoints: (1) the organizational role of IS security, (2) research objectives, and (3) research approach and theoretical background. The analysis is summarized in Table 4.

Table 4. Summary of the existing IS security awareness research.

IS awareness approach	Org. role of IS security	Research objectives	Research approach	Theoretical background
Cognitive approaches				
Aytes and Connolly (2003)	Social	Interpretive	Conceptual analysis	Human perception of risk (Slovic 1987), humans' reactions to risks (e.g., Fischhoff, Slovic, & Lichtenstein 1978, Fischhoff, Slovic, Lichtenstein, Read & Combs 1979, Zeckhauser & Viscusi 1990) and people's general attitude towards risk (e.g., Weber & Milliman 1997).

IS awareness approach	Org. role of IS security	Research objectives	Research approach	Theoretical background
Banerjee, Cronan and Jones (1998)	Social	Interpretive	Theory-testing	The theory of reasoned action (Fishbein & Ajzen 1975), the theory of planned behavior (Ajzen 1991) and Kohlberg's theory of moral development (Kohlberg 1981).
Barman (2002)	Technical	Means-end	Conceptual analysis	Not found
Beatson (1991)	Socio-technical	Means-end	Conceptual analysis	Not found
Bray (2002)	Socio-technical	Means-end	Conceptual analysis	Not found
Cox, Connolly and Currall (2001)	Socio-technical	Means-end	Conceptual analysis	Not found
Denning (1999)	Socio-technical	Interpretive	Conceptual analysis	Not found
Desman (2002)	Socio-technical	Means-end	Conceptual analysis	Not found
Forcht, Pierson and Bauman (1988)	Social	Interpretive	Conceptual analysis	Not found
Furnell, Gennatou and Dowland (2001, 2002)	Socio-technical	Means-end	Conceptual analysis	Not found
Gaunt (1998)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Gaunt (2000)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Hadland (1998)	Socio-technical	Means-end	Conceptual analysis	Not found
Hansche (2001a)	Socio-technical	Means-end	Conceptual analysis	Not found
Hansche (2001b)	Socio-technical	Means-end	Conceptual analysis	Not found
ISF (2005)	Socio-technical	Means-end	Conceptual analysis	Not found
Kajava and Siponen (1997)	Social	Means-end	Conceptual analysis	Not found

IS awareness approach	Org. role of IS security	Research objectives	Research approach	Theoretical background
Katsikas (2000)	Social	Means-end	Conceptual analysis	Not found
Kluge (1998)	Social	Means-end	Conceptual analysis	Not found
Kovacich (1998)	Socio-technical	Means-end	Conceptual analysis	Not found
Kovacich and Halibozek (2003)	Socio-technical	Means-end	Conceptual analysis	Not found
Lafleur (1992)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Markey (1989)	Socio-technical	Means-end	Conceptual analysis	Not found
Martins and Eloff (2002)	Socio-technical	Means-end, interpretive	Theory-testing	Not found
McLean (1992)	Socio-technical	Means-end, interpretive	Conceptual analysis	The stimulus-response model (e.g., Skinner 1991), model of the adoption of innovations (Rogers 1962)
Murray (1991)	Socio-technical	Interpretive	Conceptual analysis	Not found
NIST (1996)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
NIST (1998)	Social	Means-end, interpretive	Conceptual analysis	Not found
NIST (2003)	Social	Means-end, interpretive	Conceptual analysis	Not found
Peltier (2000, 2002)	Socio-technical	Means-end	Conceptual analysis	Not found
Proctor and Byrnes (2002)	Socio-technical	Interpretive	Conceptual analysis	Not found
Rudolph, Warshawsky and Numkin (2002)	Socio-technical	Means-end	Conceptual analysis	Not found
Schlienger and Teufel (2002)	Socio-technical	Interpretive	Conceptual analysis	Not found
Siponen (2000c)	Social	Means-end, interpretive, critical	Conceptual analysis	The principle of the “veil of ignorance” (Rawls 1999), Hare's overriding thesis (Hare 1981)
Spurling (1995)	Social	Means-end	Conceptual analysis	Not found

IS awareness approach	Org. role of IS security	Research objectives	Research approach	Theoretical background
Stacey (1996)	Social	Means-end, interpretive	Conceptual analysis	Not found
SSE-CMM (1999)	Socio-technical	Means-end	Conceptual analysis	Not found
Telders (1991)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
I^2SF (1999)	Socio-technical	Means-end	Conceptual analysis	Not found
Thomson and von Solms (1998)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Vroom and von Solms (2002)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
White House (2003a, 2003b)	Social	Interpretive	Conceptual analysis	Not found
Wood (2002)	Socio-technical	Interpretive	Conceptual analysis	Not found
Behavioral approaches				
Parker (1998, 1999)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Cognitive and behavioral approaches				
Furnell, Sanders and Warren (1997)	Socio-technical	Interpretive	Conceptual analysis	Not found
ISO (2005)	Socio-technical	Means-end	Conceptual analysis	Not found
Kabay (2002)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Mitnick (2002)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Perry (1985)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Pipkin (2000)	Socio-technical	Interpretive	Conceptual analysis	Not found
Sasse, Brostoff and Weirich (2001)	Socio-technical	Interpretive	Theory-creating	Not found

IS awareness approach	Org. role of IS security	Research objectives	Research approach	Theoretical background
Siponen (2000a)	Socio-technical	Means-end, interpretive, critical	Conceptual analysis	The theory of reasoned action (Fishbein & Ajzen 1975), the theory of planned behavior (Ajzen 1991), intrinsic motivation (Deci & Ryan 1985), the principle of "veil of ignorance" (Rawls 1999), Hare's overriding thesis (Hare 1981), and the technology acceptance model (Davis 1989).
Straub (1990)	Technical	Means-end, interpretive	Theory testing	The theory of general deterrence (Blumstein, Cohen & Nagin 1978)
Straub, Carlson and Jones (1993)	Technical	Means-end	Theory testing	The theory of general deterrence (Blumstein, Cohen & Nagin 1978)
Straub and Welke (1998)	Technical	Means-end, interpretive	Theory testing	The theory of general deterrence (Blumstein, Cohen & Nagin 1978)
Thomson and von Solms (1997)	Socio-technical	Means-end, critical	Conceptual analysis	Not found
Tudor (2001)	Socio-technical	Means-end, interpretive	Conceptual analysis	Not found
Wood (1995)	Socio-technical	Means-end	Conceptual analysis	Not found
The approach is unspecified				Not found
Vyskoc and Fibikova (2001)	Socio-technical	Interpretive	Theory-creating	Not found

The means that are proposed by the existing research to influence on users' security behavior can be classified into two categories: (1) cognitive approaches and (2) behavioral approaches. However, as stated earlier, a combination of several IS security awareness approaches is expected to be more efficient than using a single approach in isolation. Sharing this viewpoint, 15 of the analyzed 59 studies proposed a combination of cognitive and behavioral IS security awareness approaches.

The analysis of the existing IS security awareness research concludes with a consideration of the two categories. Cognitive approaches are taken up first and then behavioral approaches. Finally, the implications for future research and practice are discussed.

The existing research and cognitive approaches

Cognitive approaches consider the individual as an active processor of the information he receives and consequently, that his behavior is not changed unless he understands the information in a meaningful way. In the existing IS security awareness research, cognitive approaches aim to improve users' behavior through (i) persuasive communication and (ii) active participation in the design of IS security measures.

The majority of *cognitive approaches* aspire to change users' security behavior by means of *training.* In addition to persuasive communication explaining why compliance with IS security instructions is necessary, training involves the teaching of the knowledge and skills that are required to enable such compliance. In the existing research, several training media are utilized such as lectures (e.g., Hansche 2001a, 2001b, Kovacich 1998), personal discussions (e.g., Cox *et al.* 2001), videos (e.g., Hadland 1998, Hansche 2001a), a variety of printed materials (e.g., Hadland 1998, Hansche 2001a, Kovacich 1998), and computer- and web-based systems (Hansche 2001a, 2001b, Furnell *et al.* 2001, 2002).

In addition to training, *IS security campaigns* (McLean 1992) and *personal example shown by IS security experts and management* (e.g., Gaunt 2000, Martins & Eloff 2002) are used as a means to persuasive communication. Furthermore, *active participation* is put into practice by involving users in the design of information policies and instructions (e.g., Gaunt 1998).

Most of the studies proposing *IS security awareness training* take a socio-technical perspective on the role of IS security and have means-end research objectives. However, they are often compromised by two shortcomings. First, they do not present their underlying theories. In consequence, practitioners lack knowledge as to why the suggested IS security awareness approaches are expected to improve users compliance with IS security policies and instructions. Second, as the prevailing research approach is conceptual analysis, empirical evidence on the practical efficiency of training is not presented.

One of the analyzed studies proposes utilizing *security campaigns* (McLean 1992). The study offers means aimed at changing user behavior. It demonstrates a socio-technical perspective on the organizational role of IS security, has interpretive and means-end research objectives, and as theory, utilizes the stimulus-response model (cf., Skinner 1991 p. 9) and the adoption of innovations model (Rogers 1962). Furthermore, the study employs conceptual analysis as its research approach and hence does not empirically explore the practical efficiency of security campaigns.

Two of the analyzed awareness approaches (Kabay 2002, Thomson & von Solms 1998) propose the use of principles of *social psychology* as a means (e.g., through persuasive communication) to improve users' security behavior. These two studies do not present theories underlying them. The study by Kabay (2002) has means-end and interpretive research objectives and Thomson and von Solms (1998) have interpretive and critical research objectives. Both studies employ conceptual analysis as their research approach. Hence, empirical evidence on the practical effectiveness of social psychology in the context of IS security is not provided.

Four studies (Forcht *et al.* 1998, Kluge 1998, Siponen 2000a, 2000c) propose the use of *morals and ethics* (e.g. via persuasive communication) to affect users' attitudes and

behavior. The study by Forcht *et al.* (1988) takes a social viewpoint of IS security and has interpretive research objectives. In addition, it utilizes conceptual analysis, but does not present its theoretical underpinnings. Kluge (1998) has a social perspective on the organizational role of IS security and means-end research objectives. The study employs conceptual analysis, but does not present the theoretical background of the proposed IS security awareness approach. Siponen (2000a) and Siponen (2000c) utilize the following ethical theories: (1) the principle of the "veil of ignorance" (Rawls, 1999) and (2) Hare's overriding thesis (cf., Hare 1981). Furthermore, the organizational role of IS security is seen in Siponen (2000a) as socio-technical and in Siponen (2000c) as social. Both studies have means-end oriented, interpretive and critical research objectives and employ conceptual analysis.

Six studies, Gaunt (1998), Gaunt (2000), Lafleur (1992), Schlienger and Teufel (2002), Spurling (1995), and Telders (1991) propose *active participation in the design of IS security measures.* Of these approaches, Gaunt (1998, 2000), Lafleur (1992), and Telders (1991) take a socio-technical perspective on the role of IS security, have means-end and interpretive research approaches, and employ conceptual analysis without presenting the theoretical background of their approaches. Schlienger and Teufel (2002) also envisage a socio-technical organizational role of IS security. In addition, the study has interpretive research objectives and it employs conceptual analysis without explicitly presenting its theoretical background. Spurling (1995) sees IS security as having a social organizational role, has means-end and interpretive research objectives and employs conceptual analysis without presenting the theoretical background of the proposed IS security awareness approach.

The existing research and behavioral approaches

Behavioral approaches are based upon the idea that changes in behavior are the result of manipulating environmental variables in response to undesirable behaviors. In the context of IS security, this means *punishing* violations against (e.g., Parker, 1998, 1999) and *rewarding* compliance with (e.g., Kabay 2002, Parker, 1998, 1999) IS security instructions.

Straub (1990), Straub *et al.* (1993) and Straub and Welke (1998) present theoretical background and empirical evidence to the effectiveness of *deterrence*. These three studies are theory-testing. Straub (1990) and Straub and Welke (1998) have interpretive and means-end oriented and Straub *et al.* means-end oriented research objectives. Additionally, Straub (1990) and Straub *et al.* (1993) have a technical and Straub and Welke (1998) a socio-technical viewpoint of IS security. Other studies also propose using punishment, however without exploring it in practice. The latter include Furnell *et al.* (1997), ISO (2005), Mitnick (2002), Siponen (2000a), Thomson and von Solms (1997), Tudor (2001), and Wood (1995). These studies have a socio-technical standpoint. Moreover, the studies have means-end research objectives. In addition, Mitnick (2002) and Tudor (2001) have interpretive, Siponen (2000a) interpretive and critical, and Thomson and von Solms (1997) critical research objectives. All of the studies employ conceptual analysis and do not present the theoretical background to their proposals of the use of punishment.

Kabay (2002), Mitnick (2002), Parker (1998, 1999), Perry (1985), Siponen (2000a) and Sasse *et al.* (2001) propose the use of *rewards* in order to improve users' security behavior. These studies take a socio-technical view of the role of IS security. Kabay (2002), Mitnick (2002), Parker (1998, 1999), Perry (1985), and Siponen (2000a) employ conceptual analysis. In addition, Sasse *et al.* (2001) is a theory-creating study. No one of these studies presents the theoretical background for proposing rewards to compliance with IS security policies and instructions.

Implications of the analysis for future research and practice

Future research should address the shortcomings pointed out by the present analysis of the literature. The dominant research approach was conceptual analysis. It was utilized by 53 of the existing IS security awareness studies. Hence, empirical evidence for the effectiveness of the various IS security awareness approaches was not presented, except those concerned with deterrence. Consequently, practitioners do not have information on the effectiveness of the existing IS security awareness approaches on hand. In addition, the theoretical background of the approaches was seldom presented. This was done in seven of the analyzed studies. Explaining the theoretical background would be useful for practitioners as it helps to understand why a particular approach is expected to have the desired impact on users' security behavior. In addition, the need to use appropriate theories in the IS discipline has been pointed out by scholars (e.g., Walls *et al*. 1992).

On the basis of the results of the analysis, theory-based IS security awareness approaches are called for. In addition, their practical effectiveness should be explored. The need for further empirical evidence is apparent with respect to all the cognitive approaches. Of the behavioral approaches, especially the practical effectiveness of rewards has not been empirically explored in the context of IS security (see also Siponen, 2000b p. 206). Hence, empirical studies of rewards would be welcomed.

4 Three design theories for IS security awareness

As mentioned earlier, IS security solutions lose their usefulness, if users do not follow them (Siponen 2000a p. 31, 2000b p. 197, 2001 p. 26, Ølnes 1994 p. 632). Hence, effective IS security requires that users are not only aware, but also comply with their security mission as described in their organizations' security policies.

To make users capable and motivated to follow IS security instructions, 59 different IS security awareness approaches have been proposed by scholars and IS security practitioners. As pointed out in the previous chapter, most of the approaches are neither based on theories nor empirically validated in practice[1]. In this chapter, the aim is to sketch three IS security awareness approaches that address these two concerns. To achieve this aim, we see the concept of design theorizing, first elaborated by Walls *et al.* (1992) and further modified by Hevner, March, Park and Ram (2004) as a fruitful approach.

According to the concept of design theorizing, an IS security awareness program (1) is based on appropriate kernel theories, (2) offers concrete guidance on how to achieve behavioral change towards acceptance of IS security policies and instructions, and (3) set a testable research agenda for scholars (Walls *et al*. 1992, Markus, Majchrzak & Gasser 2002). After pointing out the limits of the existing IS security approaches in the light of the above three criteria, we propose three alternative strategies to build a successful IS security awareness program that meets these criteria.

The rest of this chapter is organized as follows. In section 4.1, properties of design theories are presented. In section 4.2, the existing awareness approaches are analyzed using the aforementioned three criteria. Section 4.3 proposes three awareness approaches that satisfy these criteria. Finally, the implications for research and practice are discussed in section 4.4.

[1] This has also been noted by scholars among whom Aytes and Connolly (2003) and Siponen (2000a) have criticized existing IS security awareness approaches to lacking (i) theoretically grounded and (ii) testable concrete guidance to ensure that users are committed to fulfilling their IS security mission. The body of literature referred to in these studies, however, includes less than 10 IS security awareness approaches.

4.1 Properties of design theories

Design theories aim to support reaching a certain goal, and thus are prescriptive, while social science and natural science theories are typically exploratory or predictive (Walls *et al*. 1992 p. 40). However, a design theory may include kernel theories from natural and social sciences. Although, a technology-based artifact (e.g., a design theory for designing software) is a typical example of the application of design theory, organizational design activities, such as work practices and policies are also regarded as design theory activities (Hevner *et al.* 2004 p. 77-79). Design theories have two main dimensions: a *product* and a *process* (Figure 2). The *product* refers to a set of properties that a product should have for achieving a certain goal, while the *process* prescribes the method for constructing the product (Walls *et al*. 1992 p. 41).

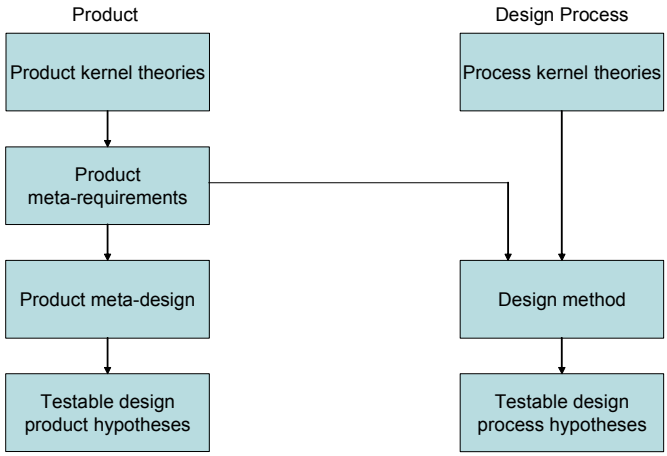

Fig. 2. Components of a design theory (Walls et al. 1992 p. 44): product and design process.

The first aspect of a design theory deals with the product. The meta-requirements of the product are derived from the relevant kernel theories (Walls *et al*. 1992 p. 42). Meta-requirements describe the goals to which the design theory applies. The meta-design describes a set of design principles hypothesized to meet the meta-requirements (Figure 2). Finally, a set of testable product hypotheses are used to verify whether the design satisfies the requirements (Walls *et al*. 1992 p. 42-43).

The second aspect of a design theory deals with the design process that incorporates the kernel theories governing that process. The design method describes the procedures for constructing the product. Finally, a set of testable design process hypotheses are used to verify whether the design method results in a product which is consistent with the design of the product. (Walls *et al*. 1992 p. 42)

4.2 The existing IS security awareness approaches from the perspective of design theory

Next, the existing IS security awareness studies that present means to influence users' behavior are analyzed from the standpoint of design theory. As argued, IS security awareness approaches should be based on (1) appropriate (kernel) theories; (2) provide concrete guidance on how to achieve behavioral change towards acceptance of IS security instructions; and (3) set a testable research agenda for scholars. Next we illustrate the extent to which the existing IS security awareness approaches attend to these three features (Table 5).

A study is regarded as based on relevant kernel theories (1) if it explicitly presents the use of such theories. Additionally, the criterion of concrete guidance (2) is met when the study presents a systematic approach and gives concrete advice to practitioners concerning the implementation of the proposed IS security awareness approach. Furthermore, setting a testable research agenda for scholars (3) requires that the study explicitly presents research questions to explore further the proposed IS security awareness approaches.

Table 5. Summary of the existing IS security awareness research from the viewpoint of design theorizing.

Study	Cognitive approaches		Behavioral approaches				
	Persuasive communication and training	*Active participation*	*Reward*	*Punishment*	Kernel theory	Conc. guidance	Research agenda
Aytes and Connolly (2003)	X				X		X
Banerjee, Cronan and Jones (1998)	X				X		X
Barman (2002)	X						
Beatson (1991)	X						
Bray (2002)	X						
Cox, Connolly and Currall (2001)	X						
Denning (1999)	X						
Desman (2002)	X					X	
Forcht, Pierson and Bauman (1988)	X						

Study	Cognitive approaches		Behavioral approaches				
	Persuasive communication and training	*Active participation*	*Reward*	*Punishment*	Kernel theory	Conc. guidance	Research agenda
Furnell, Gennatou and Dowland (2001, 2002)	X						
Furnell, Sanders and Warren (1997)	X			X			
Gaunt (1998)	X	X					
Gaunt (2000)	X	X					
Hadland (1998)	X						
Hansche (2001a)	X					X	
Hansche (2001b)						X	
ISF (2005)	X						
ISO (2005)	X			X			
Kabay (2002)	X		X				
Kajava and Siponen (1997)	X						
Katsikas (2000)	X						
Kluge (1998)	X						
Kovacich (1998)	X						
Kovacich and Halibozek (2003)	X					X	
Lafleur (1992)	X	X					
Markey (1989)	X						
Martins and Eloff (2002)	X						
McLean (1992)	X				X	X	
Mitnick (2002)	X		X	X			
Murray (1991)	X						
NIST (1996)	X					X	
NIST (1998)	X					X	
NIST (2003)	X					X	
Parker (1998, 1999)			X	X			

Study	Cognitive approaches		Behavioral approaches				
	Persuasive communication and training	*Active participation*	*Reward*	*Punishment*	Kernel theory	Conc. guidance	Research agenda
Peltier (2000, 2002)	X						
Perry (1985)	X		X				
Pipkin (2000)	X			X			
Proctor and Byrnes (2002)	X						
Rudolph, Warshawsky and Numkin (2002)	X						
Sasse, Brostoff and Weirich (2001)	X		X				
Schlienger and Teufel (2002)	X	X					
Siponen (2000a)	X		X	X	X		
Siponen (2000c)	X				X	X	X
Spurling (1995)	X	X					
Stacey (1996)	X						
Straub (1990)	X			X	X	X	X
Straub, Carlson and Jones (1993)	X			X	X		
Straub and Welke (1998)	X			X	X	X	X
SSE-CMM (1999)	X					X	
Telders (1991)	X	X				X	
I^2SF (1999)	X						
Thomson and von Solms (1997)	X			X		X	
Thomson and von Solms (1998)	X						
Tudor (2001)	X			X		X	
Vroom and von Solms (2002)	X					X	

Study	Cognitive approaches		Behavioral approaches				
	Persuasive communication and training	*Active participation*	*Reward*	*Punishment*	Kernel theory	Conc. guidance	Research agenda
Vyskoc and Fibikova (2001)	Not specified	Not specified	Not specified	Not specified			
White House (2003a, 2003b)	X						
Wood (2002)	X					X	
Wood (1995)	X		X	X			

Kernel theories

The theoretical background of existing IS security awareness studies was analyzed in section 3.3.3. However, a brief recapitulation of this issue is presented in this section. Only those IS security awareness studies mentioned below are based on kernel theories. The other approaches do not explicitly present their theoretical background.

The study by Aytes and Connolly (2003) is based on Slovic's study regarding human perception of risk (Slovic 1987). In addition, the model utilizes the results of the existing research regarding humans' reactions to risks (e.g., Fischhoff *et al.* 1978, Fischhoff *et al.* 1979, Zeckhauser & Viscusi 1990) and person's general attitude towards risk (e.g., Weber & Milliman 1997).

Banerjee *et al.* (1998) construct a framework for exploring situational ethical behavior. The framework is based on several kernel theories: the theory of reasoned action (Fishbein & Ajzen 1975), the theory of planned behavior (Ajzen 1991) and Kohlberg's theory of moral development (Kohlberg 1981). Moreover, McLean (1992) utilizes the stimulus-response model (e.g., Skinner 1991 p. 9) and Rogers' model of adoption of innovations (Rogers 1962).

Siponen (2000a) presents a behavioral framework based on the theory of reasoned action (Fishbein & Ajzen 1975), the theory of planned behavior (Ajzen 1991), intrinsic motivation (Deci & Ryan 1985), the principle of the "veil of ignorance" (Rawls 1999), Hare's overriding thesis (cf., Hare 1981), and the technology acceptance model (Davis 1989). In addition, Siponen (2000c) utilizes universal prescriptivism (Hare 1981) and the theory of justice (Rawls 1999). Moreover, Straub (1990), Straub *et al.* (1993) and Straub and Welke (1998) are based on the theory of general deterrence (cf., Blumstein, Cohen & Nagin 1978).

Concrete guidance

Aytes and Connolly (2003) present a testable model of user behavior, but do not present concrete means as to how that behavior can be influenced in practice.

Banerjee *et al.* (1998) propose training programs, codes of conduct, and enforcement of company policies and rules to prevent computer misuse. However, the study does not put forward a systematic way to implement them in practice.

Barman (2002) argues that training and punishment can be used to increase compliance with security policies, but does not present a way of doing it in practice.

Beatson (1991) proposes IS security awareness training to improve users' security behavior, without, however, offering guidance on its practical implementation.

Bray (2002) argues for training in order to avoid security breaches, but does not give guidance on how to set up training in practice.

Cox *et al*. (2001) examine three approaches to increasing awareness in an academic setting: discussion sessions, checklists and web based tutorials. However, the study does not give practical guidance in setting up these approaches.

Denning (1999) proposes training as a means to improve users' security behavior. The study suggests training areas such as physical and personnel security, cyberspace security, and social engineering tactics. However, it does give guidance on how to design and implement such training in practice.

Desman (2002) presents a systematic framework for building an awareness program and gives practical advice on how to deliver the program.

Forcht *et al.* (1988) suggest education as a means to increasing users' ethical awareness. However, no guidance on its practical implementation is given.

Furnell *et al.* (2001, 2002) discuss promoting security awareness within small organizations and present a prototype security training tool for this purpose. However, advice governing designing and implementing training sessions in practice is not given.

Furnell *et al.* (1997) highlight key issues in promoting training and awareness that healthcare establishments should consider in setting up training and awareness frameworks. The study presents some basic steps that could be taken to address an organization's training and awareness requirements. However, guidance on how the aforementioned steps could be implemented in practice is not presented.

Gaunt (1998) discusses installing an organizational IS security policy. The study presents principles regarding preparing and implementing the policy. In addition, it proposes means of training employees in the policy. However, the study does not give the practitioner guidance regarding the implementation of the policy and training.

Gaunt (2000) discusses practical approaches to creating a security culture. The study presents impediments to changing an organization's culture. However, the study does not give guidance regarding overcoming the impediments and achieving the desired cultural change.

Hadland (1998) deals with designing an IS security awareness campaign. The study lists matters that should be covered in a security campaign. In addition, it puts forward a code of practice for users' security. However, the study does not give advice how security campaigns can be systematically designed and implemented in practice.

Hansche (2001a) deals with a security awareness program. It presents a seven-step framework for setting up an awareness program. In addition, the study gives concrete advice to practitioners concerning the implementation of each step.

Hansche (2001b) discusses IS security training. The study presents a five-step framework for setting up information system security training. The study also gives concrete advice to practitioners regarding implementing the steps.

ISF (2005) aims to address IS security issues from a business perspective and to give a practical basis for assessing an organization's IS security arrangements. Improving users' IS security awareness through IS security training is one of the issues covered by the

standard. However, ISF (2005) fails to give practical advice on how to plan and deliver an IS security awareness training program.

ISO (2005) governs organizational issues regarding IS security management. One such issue is users' IS security awareness. However, the standard lacks guidance on improving users' awareness in practice.

Kabay (2002) discusses utilizing social psychology to achieve users compliance with IS security policies. The study discusses various principles of social psychology and lists some ideas for practitioners in seeking to achieve users compliance with IS security policies according to these principles. However, guidance on how to implement these ideas systematically in practice is not given.

The study of Kajava and Siponen (1997) discusses IS security awareness in the context of a Finnish university. The study lists principles regarding a security awareness program and methods for awareness, but fail to offer guidance for practitioners regarding planning and implementing the program in practice.

Katsikas (2000) presents a methodology for determining the training needs of personnel classes within health care establishments with respect to IS security and applies the methodology to determine the training needs of managers. Furthermore, the study lists the contents of training for managers. However, concrete guidance to practitioners on how to plan and deliver the training is not presented.

Kluge (1998) discusses a model code of ethics for health information professionals as a means to protect sensitive electronic information about patients. The study lists principles for a model code of ethics, but does not give guidance to practitioners on how the principles should be implemented.

Kovacich (1998) gives an overview of an IS security awareness program. The study presents valuable facts about the program (e.g., segmenting the audience according to various groups of IS users). In addition, it argues for awareness briefings and dedicated awareness material and lists several types of awareness material. However, concrete guidance to practitioners on planning and implementing awareness sessions and material is not given.

Kovacich and Halibozek (2003) address the need for IS security awareness training and discusses the basic elements of a training program along with processes and procedures for development, acquisition, and delivery of the training. The study outlines a plan for a training program and gives concrete guidance on how to set up such program in practice.

Lafleur (1992) deals with training as a part of a security awareness program. The study states the objectives for successful training: to get employees to understand the importance of their role in IS security solutions. However, concrete guidance how to systematically set up a training program that helps to achieve employees' understanding is not given.

Markey (1989) discusses training as a means of making the organization aware and involved in computer security through on-going training and awareness programs. The study argues for seminars and briefings as a means to achieve this situation. However, it does not give concrete guidance on planning and delivering the seminars.

Martins and Eloff (2002) discuss the concept of IS security culture and an assessment approach developed to implement and improve such culture. However, the level of

abstraction of the concept remains high without any concrete guidance to practitioners regarding means of fostering a security culture.

McLean (1992) discusses some marketing concepts that can be used in designing and structuring an IS security awareness program. The study puts forward a five-step systematic framework to set up such program. In addition, the study gives concrete guidance to practitioners how to plan and implement each particular step.

Mitnick (2002) presents an overview of creating training and awareness program. The overview deals with the structure and contents of such program, but does not give concrete guidance to practitioners concerning the design and implementation of the program.

Murray (1991) presents examples of security awareness programs. The study argues that such programs should be targeted at all employees who have contact with information technology assets. It also proposes means to deliver the programs. However, concrete guidance regarding planning and delivering the programs is not given.

NIST (1996) presents a seven-step approach for developing an IS security awareness training program and gives concrete guidance to practitioners regarding the implementation of each step.

In the same vein, NIST (1998) presents a methodology for setting up a role-based IS security awareness training program. The study also gives guidance on how to set up such program in practice.

Also NIST (2003) puts forward four critical steps in the life cycle of an information technology security awareness and training program and gives concrete guidance on identifying training needs, developing a training plan, getting funding for the training program, selecting training topics, finding sources of training material, implementing training material, evaluating the effectiveness of the program, and updating and improving the program. Hence, the study succeeds in giving concrete guidance to practitioners.

Parker (1998, 2000) deals with motivating end users for IS security. The studies list motivational factors and argue for rewards and penalties. In addition, they suggest various forms of awareness material. In addition, an action plan for motivation is presented. However, the studies lack guidance on how to systematically set up a motivational program in practice.

Peltier (2000, 2002) discusses implementing a security awareness program. The studies present an overview of security awareness program development and methods to convey the awareness message. They also propose practices for implementing a security awareness program as well as several media for delivering the message of the program. However, Peltier (2000, 2002) lacks guidance for practitioners on how to systematically plan and implement an IS security awareness program.

Perry (1985) discusses creating enthusiasm for computer security through (1) creating a supportive environment and (2) initiating action to create individual enthusiasm. The study lists various means to achieve these two goals. However, practical guidance for systematic implementation of the proposed means is not given.

Pipkin (2000) argues for employee training in order to increase their IS security awareness. However, the study does not describe how to implement such training in practice.

Proctor and Byrnes (2002) suggest that basic marketing techniques are relevant in designing an IS security awareness program. However, the study does not present any specific techniques in this area. Hence, it lacks guidance on how to design an IS security awareness program in practice.

Rudolph *et al. (*2002) sketch a security awareness program that targets improving users' IS security awareness. The program is implemented via a media campaign. The study proposes the campaign contents and various techniques for presenting the contents. However, the study lacks guidance to practitioners on how to systematically develop and deliver IS security awareness training and campaigns.

Sasse *et al.* (2001) suggest some means to add to users' knowledge about IS security and motivate them to protect information. For this purpose, the study proposes the use of training, punishment and reporting security-related incidents. However, advice how to implement the proposed means in practice is not given.

Schlienger and Teufel (2002) argue that that exemplary behavior on the part of managers, security training of employees, and the awarding of behavior which conforms to security practices are means to foster a security culture. However, the study does not explain how to implement the proposed means in practice.

Siponen (2000a) presents a framework for persuasive approaches based on morals and ethics, well-being, a feeling of security, rationality, logic and emotions. However, the study does not give concrete guidance to practitioners regarding the implementation of the framework.

Siponen (2000c) argues that human morality exerts a role in terms of security, and he proposes using it as a means of protection. He also puts forward a two-step approach on the use of morals and ethics as a means of information protection. Hence, Siponen (2000c) gives concrete guidance for practitioners.

Spurling (1995) discusses promoting security awareness and users commitment to IS security. The study presents several means for delivering the security awareness message, but without guidance to implement the aforementioned means in practice.

Stacey (1996) presents a tool for evaluating the maturity of an organization from the perspective of IS security. The tool consists of five stages of maturity. The study argues that training is an important means to achieve high levels of maturity. However, it does not give guidance on how to set up training in practice.

Straub (1990) argues that IS security deterrents result in a reduction in the incidence of computer abuse. The study puts forward a systematic, four-stage approach on actions to be taken in order to achieve a reduced number of abuses and gives concrete guidance to practitioners on its implementation.

Straub *et al.* (1993) give guidance on how managers could achieve a reduced number of computer abuses. However, concrete guidance on how to utilize the proposed means (e.g., meetings, training sessions, security software packages) is not given.

Straub and Welke (1998) present an approach to be used to make managers aware of actions they can take to reduce risks. The study gives concrete guidance on changing an organization’s security environment by outlining a four-phase framework for managers. In addition, the study proposes a concrete action plan for each phase.

SSE-CMM (1999) puts forward an eight-step framework for a systematic design process for IS security awareness training. In addition, the study gives advice on setting up a training program in practice.

Telders (1991) presents a systematic approach to designing an IS security awareness program and gives concrete suggestions to practitioners regarding the implementation of the framework.

I^2SF (1999) includes IS security awareness as an important subject. However, the study does not give guidance on improving users' IS awareness in practice.

Thomson and von Solms (1997) deal with the need for an IS security awareness program in an organization. The study suggests techniques on how to implement the program in practice. However, it does not give concrete guidance on how to systematically build an awareness program that utilizes the proposed means. ´

Thomson and von Solms (1998) discuss the use of social psychology in security awareness training. The study gives some suggestions as to how the principles of social psychology could be used to improve the effectiveness of training. However, it lacks guidance on systematic implementation of the proposed principles in practice.

Tudor (2001) puts forward a systematic ten-step approach to developing an IS security awareness training program and gives concrete guidance to practitioners on utilizing the framework in developing an IS security awareness training program.

Vroom and von Solms (2002) present a seven-step framework for developing an IS security awareness program. In addition, the study gives guidance to practitioners on developing an IS security awareness program that utilizes an IS security awareness website.

Vyskoc and Fibikova (2001) suggest unnamed management techniques to influence users' behavior, values and habits. Hence, the means that the study proposes for improving users' security behavior are not identified. Consequently, the study does not give concrete guidance on how to influence user behavior.

White House (2003a, 2003b) describes a program by the US government to promote a national IS security awareness and training program and offers actions and recommendations for such program. However, advice is not given on how to systematically implement the actions and recommendations in practice.

Wood (2002) presents a security education campaign that aims at helping managers and employees to change attitudes and behavior towards the improvement of protection for critical information assets. In addition, the study puts forward a practical – but brief – seven-step action plan to implement the campaign.

Wood (1995) provides a list of 53 practical awareness raising methods that are grouped by the type of communication involved. However, the study does not give guidance on utilizing the proposed means in practice.

To conclude, Desman (2002), Hansche (2001a, 2001b), Kovacich and Halibozek (2003), McLean (1992), NIST (1996), NIST (1998), NIST (2003), Siponen (2000c), Straub (1990), Straub and Welke (1998), SSE-CMM (1999), Telders (1991), Thomson and von Solms (1997), Tudor (2001), Vroom and von Solms (2002), and Wood (2002) give concrete guidance on achieving a behavioral change towards acceptance of IS security policies and instructions.

Research agenda

Aytes and Connolly (2002) put forward several questions to be investigated regarding the relationship between users' knowledge and perceptions and their behavioral choices. Hence, the study sets a testable research agenda for scholars.

Banerjee *et al.* (1998) propose a research agenda for scholars. The study puts forward several research questions towards explaining situational ethics and behavior in the information technology context.

Barman (2002) does not present any research questions for empirical exploration of increased user compliance with security policies. Similarly, Beatson (1991) does not offer research questions for further exploration of IS security awareness training. The same applies to Bray (2002). The study by Cox *et al.* (2001) too lacks a testable research agenda for scholars. Furthermore, Denning (1999), Desman (2002) and Forcht *et al.* (1988) lack a testable research agenda. Furnell *et al.* (2001, 2002) present issues covering the further development areas of their prototype security training tool. However, the study does not propose research questions for further exploration of IS security awareness training utilizing the prototype tool. In the same vein, Furnell *et al. (*1997), Gaunt (1998), Gaunt (2000), Hansche (2001a) and Hansche (2001b) lack a concrete testable research agenda for scholars. ISF (2005) does not present research questions for further exploration of IS security awareness training. The same applies to ISO (2000). In addition, Kabay (2002) lacks a research agenda for scholars. Likewise, the study by Kajava and Siponen (1997) does not put forward a testable research agenda. The same applies to Katsikas (2000), Kluge (1998), Kovacich (1998), Kovacich and Halibozek (2003), Lafleur (1992), Markey (1989), Martins and Eloff (2002), McLean (1992), Mitnick (2002), Murray (1991), NIST (1996, 1998, 2003), Parker (1998, 2000), Peltier (2000, 2002), Perry (1985), Pipkin (2000), Proctor and Byrnes (2002), Rudolph *et al.* (2002), Sasse *et al.* (2001), Schlienger and Teufel (2002), and Siponen (2000a).

Siponen (2000c) presents several issues for further exploration of human morality as means of protection and proposes conceptual analysis and empirical (theory testing/theory creating) research as possible research strategies. Hence, Siponen (2000c) sets a research agenda for scholars. In contrast, Spurling (1995) and Stacey (1996) lack a research agenda.

Straub (1990) proposes a research agenda for scholars. The study presents several issues for further exploration of ways of reducing computer abuse through the aid of deterrence. The suggestions include alternative research methods, different time frames, and different settings. Furthermore, studies with stronger checks for internal validity (field and laboratory experiments), qualitative research, and case studies are suggested as possible new directions for research in order to enhance the perspective. However, the study by Straub *et al.* (1993) lacks a testable research agenda for scholars.

Straub and Welke (1998) propose several topics with regard to further exploration of actions for managing system risks: generalizability of the findings, long-lasting effects of the explored interventions, and testing the viability of theory-based security planning in other contexts. Longitudinal studies, field experiments and additional action research are proposed as possible research strategies. The study also proposes further studies on the

general concept of risk in the computer security arena. Consequently, Straub and Welke (1998) present a research agenda for scholars.

SSE-CMM (1999) does not present research questions for further exploration of IS security awareness training. Similarly, Telders (1991) and I^2SF (1999) lack a testable research agenda for scholars. The same applies to Thomson and von Solms (1997), Thomson and von Solms (1998), Tudor (2001), Vroom and von Solms (2002), Vyskoc and Fibikova (2001), White House (2003a, 2003b), Wood (2002), and Wood (1995).

To conclude, Aytes and Connolly (2003), Banerjee *et al.* (1998), Siponen (2000c), Straub (1990), and Straub and Welke (1998) set out a testable research agenda for scholars. Thus, only three studies, Siponen (2000c), Straub (1990) and Straub and Welke (1998), fulfill all three criteria set for design theorizing.

Towards design theories for IS security awareness

As pointed out by the present literature analysis (chapter 3), in the case of IS security awareness, there is empirical evidence only on the practical efficiency of deterrence. However, empirical evidence on the practical efficiency of training, campaigns and reward in other fields suggest that these approaches have potential in improving users' IS security awareness. For example, training has been found useful in AIDS prevention (Korschun 1998), while campaigns have proven successful in changing human behavior e.g., in the context of highway safety (Rodriguez & Anderson-Wilk 2002). Similarly, rewards have for long been considered effective on human attitudes and behavior (e.g., Festinger & Carlsmith 1959).

In addition to the above, successful IS security requires that IS security policy and instructions are accepted and followed by most of the organization's employees. IS security can not be substantially enhanced by changing only a few individuals' behavior. Such wide change requires that organizational resistance – which is possible during the change process – can be dealt with. Also for this purpose training, campaigns, punishment and rewards are proposed (cf., Kotter & Schlesinger 1979), but their practical efficiency is not explored in the context of IS security awareness. Hence, recognizing the lack of adequate consideration given of training, campaigns, reward and punishment (see chapter 3), there is a need for future research on them. Accordingly, this chapter focuses on these four areas: (1) training, (2) campaigns, (3) reward and (4) punishment. Due to their same theoretical background – operant conditioning (cf. Skinner 1991) – as well as the need for an appropriate balance between the use of punishment and reward (cf., Simms & Lorenzi 1991 p. 81), these two IS security awareness approaches are considered together.

4.3 Three design theories for IS security awareness

The four IS security awareness approaches presented above can be used independently. Hence, each of the approaches can be considered as an independent IS security awareness sub-system with its own design theories (and kernel theories). However, e.g., Simms and Lorenzi (1991 p. 81) have argued that there is a need for an appropriate balance between the use of punishment and reward. Consequently, in this dissertation the

aforementioned IS security awareness approaches are considered together. Following up this idea, three design theories for IS security awareness are presented: (1) training (section 4.3.1), (2) security campaigns (section 4.3.2), and (3) reward and punishment (section 4.3.3). Similar work needs to be done on how to involve employees in the design of security measures. However, this is beyond the scope of this dissertation.

4.3.1 Design theory for IS security awareness training

This section discusses IS security awareness training whose intention is to improve users' IS security behavior towards compliance with IS security policies and instructions. For this purpose, kernel theories along with the corresponding product meta-requirements, product meta-design and testable design product hypothesis are described. Moreover, process kernel theories, the design method, and testable design process hypotheses are presented (Table 6).

Table 6. Design theory features for IS security awareness training.

Design theory features	
Design product	
Kernel theories	KT1: Universal constructive instructional theory KT2: Elaboration likelihood model
Meta-requirements	MR1: IS security awareness training should take the learner's previous knowledge into account (KT1). MR2: IS security awareness training should take the possibilities and constraints caused by the learning task, learning environment and organizational setting into account (KT1). MR3: IS security awareness training should enable systematic, cognitive processing of information (KT2). MR4: IS security awareness training should motivate for systematic, cognitive processing of information (KT2).
Meta-design	MD1: Set an awareness program that incorporates IS security awareness training with situated learning task and learning environment and pays attention to MR1-MR4.
Testable design product hypotheses	H1: IS security awareness training increases user compliance with IS security instructions.
Design process	
Kernel theories	KT1: Universal constructive instructional theory KT2: Elaboration likelihood model
Design method	1) Instructional task is defined, 2) current state of the learners is defined, 3) learning task and learning environment are reconstructed, and 4) effectiveness of the instruction is measured.
Testable design process hypothesis	PH1: It is feasible for practitioners to set up training that meets MR1-MR4 and MD1.

Design product

Kernel theories of IS security awareness training

IS security awareness training consists of two kernel theories: (1) the universal constructive instructional theory (UCIT) and (2) the elaboration likelihood model.

Kernel theory 1: Universal constructive instructional theory

Learning can be defined as a persisting change in the learner's performance – e.g., in a user's IS security behavior (Driscoll 2000 p. 3). IS security awareness training should aim at such behavioral changes. Intentional and organized opportunities for goal-directed learning can be provided through the aid of instruction. However, "*learning is such a complex matter that it might be impossible to conceive of a single theory broad enough to encompass all important aspects of learning and yet specific enough to be useful for instruction"* (Driscoll 2000 p. 399). Each individual theory can provide only a partial picture of learning, one that underlines some aspects but lacks others (Driscoll 2000 p. 399). The usefulness of the different theories varies as a result of organizational factors like employees' skills and motivation as well as the learning facilities available. Therefore, the need for customized instruction-based approaches is evident. To address this need, Schott and Driscoll (1997) have developed a framework for creating situated instructional theories; this is called *the universal constructive instructional theory* (UCIT).

Unlike traditional instructional design theories that help to design instruction itself (e.g., Gagne 1985, Glaser 1971, Dick & Carey 1996), UCIT provides a framework for designing situational instructional theories to be used in creating customized instruction. In the design process, the theory and the corresponding instruction are fitted to a certain instructional task in a certain learning environment for a certain group of learners. As argued, such an approach is necessary for efficient organizational instruction. By this token, UCIT is selected as a kernel theory for IS security awareness training.

UCIT is not intended to create a general theory. Rather, it considers the architectonics of an instructional theory as a heuristic process. Such a theory can not be found inductively after empirical experiments (Schott & Driscoll 1997 p. 138). Instead, it is constructed in a design process in which the different building blocks of the architectonics of the instructional theory are assembled.

UCIT consists of three elements: (1) functions, (2) basic components, and (3) situated possibilities/constraints systems (SPC systems) (Schott & Driscoll 1997 p. 146-156). The functions are (a) acquisition, (b) storage, and (c) use of knowledge and they concern both the learner and the learning environment. The basic components comprise four types of components: (i) the learning environment, including teacher, teaching methods and the media, (ii) the learning task, (iii) the learner, and (iv) the frame of reference where the instruction takes place (i.e., a certain social or organizational setting). Whereas the learner, the learning task, and the learning environment can be modified, the frame of reference is typically not manipulated for instructional purposes

What is learned by the learner is influenced by possibilities and constraints arising out of the available knowledge stored as external information (e.g., printed material,

computer based systems) and as internal information (e.g., the learner's previous knowledge). In addition, learning can be affected by possibilities and constraints which are based on the instructional task, the learning environment, and the frame of reference (Scott & Driscoll 1997 p. 141). All possibilities and constraints concerning a certain task in a certain teaching-learning environment establish the corresponding situated possibilities/constraints system (Scott & Driscoll 1997 p. 141). Taking essential aspects of relevant possibilities and constraints into account, the teacher reconstructs a situated learning task and the corresponding situated learning environment, including, e.g., instructor, teaching media, and teaching method (Schott & Driscoll 1997 p. 141).

Kernel theory 2: The elaboration likelihood model

An individual's cognitive processing refers to his active processing of information he receives. This contains the idea that the recipient's relevant knowledge acquisition requires him to understand the received information in a meaningful way. This enables the recipient's integration of new knowledge what he already knows. The existing research suggests that cognitive processing of persuasive information is necessary for long-lasting attitudinal and behavioral change (McGuire 1968, 1972, Greenwald 1968, Gardner 2004). However, there are other potential sources of information that the recipients of messages can base their judgments on and which do not require extensive cognitive work. The recipient can rely on a variety of cues to make quicker decisions than would be the case if he engaged in detailed cognitive processing. Cues are non-argument elements of the message that can influence attitude change without any active thinking about the issue. Hence, they allow the recipient to adopt an attitude without having to go through a deep analysis of the issue under consideration. Examples of cues are speaker credibility, reaction of others, external rewards, attractiveness of speaker, number of arguments and the amount of graphs and statistics presented.

Two attitude-change theories recognize cues as possible routes to attitude formation: the elaboration likelihood model (Petty & Cacioppo 1981, 1986) and the heuristic-systematic model (Chaiken 1980, 1987). In the elaboration likelihood model cognitive processing and cues are seen as mutually exclusive routes to persuasion whereas in the heuristic-systematic model they can happen simultaneously. Both theories point out the necessary predecessors of cognitive processing: ability and motivation. In addition, they underline what happens when people avoid thinking about the arguments they are presented with. Hence, they help instructors to focus on avoiding cues and enhancing cognitive processing. Of the two theories, the elaboration likelihood model is more widely known and referred to. Furthermore, it is based on solid empirical evidence (Petty & Cacioppo 1986). For these reasons it is chosen as the kernel theory of IS security awareness training.

The elaboration likelihood model recognizes cognitive processing (i.e., central route) and cues (i.e., peripheral route) as valid routes to attitudinal change. Attitudinal change by the central route results from detailed cognitive processing of the message. In this process, the first step is to recognize its persuasive arguments. After this, the recipient tries to understand them meaningfully. Finally, he makes an evaluation of the arguments.

Petty and Cacioppo (1981, 1986) propose that changes caused by relying on cues (i.e., following the peripheral route) are unpredictable, whereas those caused by the

cognitive processing of persuasive arguments (i.e., following the central route) are more predictable and persistent. Each recipient's cognitive processing of the arguments depends on two general factors: his motivation and his ability. A highly motivated recipient is likely to use cognitive processing. Low motivation leads to relying on cues. Petty and Cacioppo (1981, 1986) recognize three factors that have an impact on motivation: personal relevance of the topic, diversity of arguments (i.e., arguments coming from several sources), and a personal tendency to enjoy critical thinking.

Meta-requirements for IS security awareness training

As the goal of IS security instruction is to provide an opportunity for learning, the following meta-requirements concentrate on the learner's acquisition and storing of new information.

Meta-requirements derived from UCIT (KT1):

Meta-requirement 1 (MR1): IS security awareness training should take the learner's previous knowledge into account. This requirement originates in the fact that the learner's previous knowledge affects his acquisition of new information and hence his learning process. Consequently, it affects the attitudinal and behavioral changes that potentially result from the training.

Meta-requirement 2 (MR2): IS security awareness training should take possibilities and constraints caused by the instructional task, the learning environment, and the organizational setting into account. This requirement stems from the argument that the above-mentioned possibilities and constraints have an impact on the learner's acquisition of new information and thus on his learning process and potential behavioral changes.

Meta-requirement derived from the elaboration likelihood model (KT2)

Meta-requirement 3 (MR3): IS security awareness training should enable systematic cognitive processing of information. Kernel theory KT2 emphasizes the importance of cognitive processing of the persuasive information received in order to achieve persisting attitudinal and behavioral changes.

Meta-requirement 4 (MR4): IS security awareness training should motivate for systematic cognitive processing of information. Kernel theory KT2 emphasizes that the perceiver's (learner's) motivation is a necessary predecessor for his cognitive processing of information and hence for changes in his attitudes and behavior.

Meta-design features for IS security awareness training

Meta-design feature 1 (MD1): Set an awareness program that incorporates IS security awareness training with a situated learning task and environment and pays attention to MR1-MR4.

Testable design product hypothesis for IS security awareness training

Testable design product hypothesis 1 (H1): IS security awareness training increases user compliance with IS security instructions. Testing H1 involves exploring how users are able to reach the instructional goal.

Design process

Kernel theories and design process for IS security awareness training

UCIT includes a four-stage design process for instructions (Schott & Driscoll 1997 p. 162): (1) determination of the instructional goal, (2) diagnosis of the state of the learner, (3) instruction, and (4) diagnosis of success (Figure 3)

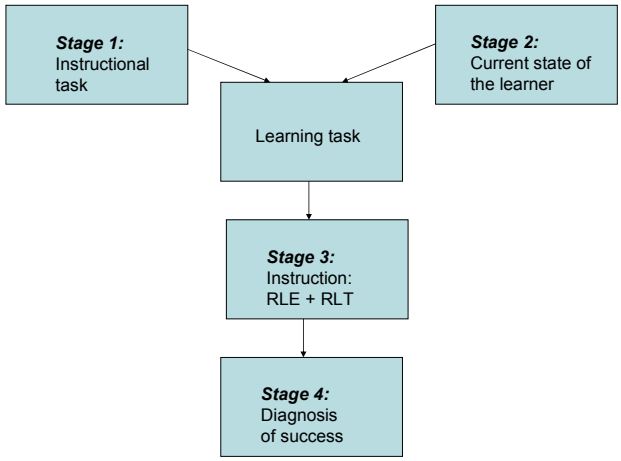

Fig. 3. Four stages of instruction (Schott & Driscoll 1997 p. 162).

The following imaginary example of a company where the sales team uses email in communication with its business partners demonstrates the instructional design process (Figure 3). The communication in the company deals with confidential information such as product prices, customer information and product information. Security audits have reported that the team follows IS security instructions well, except for improper use of email. The company's email policy states that each employee is obliged to assess the criticalness of information in his email messages and take the necessary precautions before sending a message. It stresses that confidential information must always be encrypted when it is sent via email. Despite this rule, the sales team does not encrypt any electronic messages. Hence, there is a conflict between the existing email policy and the way the team acts in reality. Applying UCIT's design process*, in the first phase* (Figure 3)*,* the instructional task is defined. In this example, the instructional task is to get the team members to follow the company's email policy.

In the second phase (Figure 3), the current state of the learners in relation to the instructional task is explored. Some of the knowledge related to the instructional task is already known by the learners, but some of it they still have to learn. The difference between the knowledge that is required and the learners' current knowledge defines what it is the learners still have to learn. This is called the learning task (Figure 3). To analyze the current state of the learners, each team member's email practice as well as the reasons for possible improper use is analyzed by interviewing the team members regarding their use of email. The analysis finds that the team members do not understand the importance of encrypting confidential information from the organization's viewpoint. In addition, they have an inadequate knowledge of the principles of classifying information. However, they are aware of the existence and contents of the email policy. In addition, they know how to use the encryption software. Hence, in our example the learning task is to give the team members the capability to classify information according to the company's IS security policy. In addition, they should understand the importance of encrypting confidential information.

In addition to lack of knowledge (e.g., contents of the email policy and information classification rules), understanding (e.g., of potential consequences of not following the instructions) and skills (e.g., using the encryption software) related to the subject matter, there may be other reasons for non-compliance with IS security instructions. In our example case, these reasons may be related to several factors, such as technology (e.g., useless encryption software), instructions (e.g., impractical email policy or information classification rules), and the work environment (e.g., work overload combined with the lack of social pressure to comply with the instructions).

In the third phase (Figure 3), the instruction – the reconstructed learning task and environment – is designed. The key is to find aspects which are vital for efficient design of the learning task and environment. The instructor should consider only those aspects which continue to act as constraints to performing the task (Schott & Driscoll 1997 p. 153). In our example, the instruction is split into two parts: (1) the importance of classifying information and (2) the importance of encrypting confidential information. Splitting the task helps learners to manage the load on their working memory (i.e., cognitive load) (cf., Clark 2003 p. 56-57) and to avoid barriers caused by a long learning task.

The first part of the instruction aims at employee learning of the company's principles of information classification. In addition, it emphasizes the importance of such classification. Learners' relevant prior knowledge should be activated before the instruction starts (Clark 2003 p. 25, 84). Examples of techniques activating prior knowledge include e.g., (Clark 2003 p. 84-85): group discussions, asking and answering pre-questions prior to learning, and presentation of a comparative advance organizer. The advance organizer contains information that is familiar to the learner and that links aspects of that familiar information to new information to be presented in the lesson (Clark 2003 p. 88).

In our example, the instruction starts with a group discussion about the threats and risks related to the use of the Internet. In addition, the discussion governs the contents of the email policy, and the reasons for encrypting valuable electronic information. Such discussion targets activation of the learners' prior knowledge related to the learning task. What follows is an instructor-led session during which the team identifies the critical

information it processes. In addition, the corresponding information classification rules are applied to this information. During this rehearsal, the instructor should give feedback that helps the learners to know the accuracy of their response and to understand the reason for it. Such feedback enhances long-lasting learning results (Clark 203 p. 128).

Next, the team estimates the impact on their own work and on the company's business if the information is unintentionally changed, lost, or revealed to hostile parties. The aim of this task is to point out the importance of information classification and proper information processing according to that classification. In addition, learners' building of such cause-and-effect mental models enhances their long-lasting learning (Clark 2003 p. 114). A further aim is to motivate cognitive — and avoid superficial — processing of information (cf., Petty & Cacioppo 1981, 1986) by making the learning task of personal relevance and consequential for the self and others. Furthermore, practical exercises that accompany lectures diminish the learners' cognitive load (Clark 2003 p. 60).

The second part of the instruction governs the specific risks related to electronic mail as well as the corresponding countermeasures. It is performed as collaborative work under supervision of an instructor. The main goal is to enhance understanding of the risks related to the use of electronic mail. Furthermore, the aim is to emphasize what the team can and should do to protect electronic information and how this can be done in practice. The collaborative tasks are targeted at the continuous use of email encryption by increasing users' cognitive processing (cf., Petty & Cacioppo 1981, 1986). Corrective feedback is necessary if long-lasting learning results are to be achieved.

In the fourth phase (Figure 3)*,* the success of instruction has to be assessed by verifying to what degree the educational goal can be reached, e.g., by exploring whether users follow the company's email policy more closely after the training. This can be done, e.g., through the aid of surveys or interviews exploring whether users themselves, their managers or peers report increased compliance with IS security instructions. During this phase, the following design process hypothesis (PH1) is tested.

Testable design process hypothesis for IS security awareness training

PH1: It is feasible for practitioners to set up training that meets MR1-MR4 and MD1 and reaches its educational goal: increased user compliance with IS security instructions.

4.3.2 Design theory for IS security awareness campaigns

In this section, IS security campaigns are discussed as a means to achieve organization-wide changes in users' security behavior. For this purpose, kernel theories for the design of IS security campaigns are presented. In addition, the corresponding meta-requirements, meta-design and testable design product hypotheses are described. Furthermore, kernel theories for the design process and the corresponding design method as well as a testable design process hypothesis are explored (Table 7).

Table 7. Design theory features for IS security awareness campaigns.

Design theory features	
Design product	
Kernel theories	KT1: Convergence model of communication
Meta-requirements	Meta-requirement 1 (MR1): Information should be shared among all communicating parties. Meta-requirement 2 (MR2): The relationships between the communicating parties must be symmetrical. Meta-requirement 3 (MR3): All communicating parties must be active during the communication process.
Meta-design	MD1: Set an awareness program that incorporates IS security campaigns and pays attention to MR1-MR3.
Testable design product hypotheses	H1: IS security campaigns increase user compliance with IS security instructions.
Design process	
Kernel theories	The convergence model of communication
Design method	Kotler's eight elements of effective marketing communication: 1) Identifying the target audience, 2) determining communication objectives, 3) designing the message, 4) selecting the communication channels, 5) establishing the budget, 6) deciding on the promotion mix, 7) measuring the promotion's results, and 8) managing the marketing communication process.
Testable design process hypothesis	PH1: It is feasible for practitioners to set up a campaign that meets MR1-MR3 and MD1 and increases user compliance with IS security instructions

Design product

Kernel theory of IS security campaigns

The communication theories of Shannon and Weaver (1949), Schramm (1954), and Berlo (1960) are commonly used as a starting point for the design of persuasive communication to be used by marketers to the target audience (cf., Fill 2002, Kotler 1997, Yeshin, 1998). These theories emphasize individual behavior at the expense of the social nature of communication. Furthermore, these theories present a linear model of communication, describing it as a one-way process from sources to receivers. However, when the aim is consensus between the communicating parties – as it is in an organizational IS security awareness campaign – a more conversational model of communication is necessary (Varey 2002 p.28). Several communication models address this need and emphasize,

instead of the effects of the sender's actions on receivers, relationships between participants (Schramm 1973), mutual understanding (Kincaid 1979, 1988) and convergence within communication networks (Rogers & Kincaid 1981).

Of the above theories, the theory of Rogers and Kincaid (1981) stresses that an individual action is not enough to achieve organization-wide change. Rather, co-operative action between the members of the organization is required to achieve common goals. This can be achieved through information sharing, mutual understanding and agreement. Such an approach is applicable to IS security issues as organizational security can not be achieved by changing the behavior of only a few individuals. A continuous dialogue between management and employees is necessary during a campaign in order to engage the whole organization into the change process (Beer & Nohria 2000). For these reasons, *the convergence model of communication* (Rogers & Kincaid 1981) is selected as the kernel theory of IS security awareness campaigns.

Kernel Theory 1: The convergence model of communication

Rogers and Kincaid (1981) state that information is something – verbal or non-verbal - that should be shared between actively participating individuals instead of just being transmitted from one party to another. In addition, they claim that information can be created by any of the communicating parties. According to the convergence model of communication (Figure 4), all communicating parties should act on the same information. Moreover, the model stresses the importance of the personal perceptions and interpretations of the communicating parties. In addition, it advocates the creation of a symmetrical relationship between the parties by sharing information. Communication is presented as a continuous process where the parties should take turns and create information to be shared, interpreted, and reinterpreted until a sufficient degree of mutual understanding and agreement is achieved to enable collective action. The outcomes of the communication process are social (mutual understanding, agreement, and collective action) and individual (perceiving, interpreting, understanding, and believing). (Rogers & Kincaid 1981, Figueroa, Kincaid, Rani & Lewis 2002 p. 4).

Each participant perceives and creates his own interpretation, understanding and beliefs about the shared information. When understanding is gained, it can be expressed to others. This creates new information, which is then (potentially) interpreted by the other parties. The initial personal understandings and beliefs gradually draw closer to each other. However, unanimity is not a necessary result: disagreement and divergence are also possible – at least when conflicts between the communicating parties' interests and values become evident. Then, further communication is necessary in order to achieve a sufficient level of mutual understanding and agreement enabling collective action and solving common problems. (Rogers & Kincaid 1981, Figueroa *et al.* 2002 p. 4-5)

At least in large organizations, it is not possible to aim at mutual understanding by engaging all employees in the conversation process. Such approach would be expensive and slow, making in unfeasible. However, an initial level of understanding between management and employees is required in order to achieve increased compliance with IS security instructions. Hence, employees should have an opportunity to give feedback. This helps management to understand the employees' viewpoint and to modify the campaign accordingly.

The feedback process should be supported by information systems. In addition, management should consider setting up a distributive discursive campaign whereby representatives of the employees present the campaign message to the other employees, collect feedback from them and present this feedback to management. In this way, employees can have a voice in organizational issues.

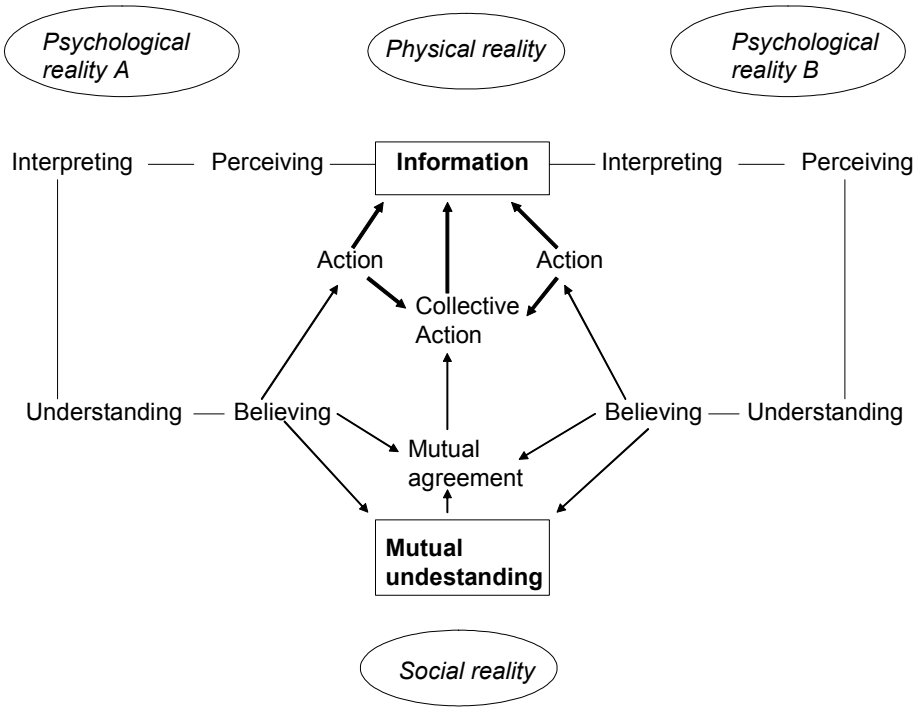

Fig. 4. The convergence model of communication (Rogers & Kincaid 1981).

Meta-requirements for IS security awareness campaigns

Meta-requirements derived from the convergence model of communication

Meta-requirement 1 (MR1): Information should be shared among all communicating parties. This requirement stems from the issue that in order to engage the whole organization in the change process the communicating parties should act on the same information. In a distributed campaign, this concerns employees' and management's representatives.

Meta-requirement 2 (MR2): The relationships between the communicating parties should be symmetrical. The convergence model of communication explicitly presents the need for symmetrical relationships between the communicating parties. This enhances organizational-wide change by ensuring that all the communicating parties have an equal

opportunity to participate in the communication process. In a distributed campaign, this concerns both employee and management representatives.

Meta-requirement 3 (MR3): All communicating parties should be active during the communication process. This requirement stems from the aim to foster mutual understanding between all the communicating parties leading to collective action. In a distributed campaign this concerns employee and management representatives.

Meta-design Features for IS security awareness campaigns

Meta-design feature 1 (MD1): Set an awareness program that incorporates IS security campaigns and pays attention to MR1-MR3.

Testable design product hypothesis for IS security awareness campaigns

Testable design product hypothesis 1 (H1): IS security campaigns increases users' compliance with IS security instructions.

Design process

Kernel theory and the process of designing IS security awareness campaigns

The convergence model of communication aims at mutual understanding and collective action. As such, it is an applicable kernel theory for use in designing an IS security awareness campaign. Several studies and textbooks present systematic approaches for designing effective marketing communication (e.g., Varey 2002, Fill 2002, Kotler 1997). These approaches are similar to each other, containing such phases as: 1) recognizing the target audience and its characteristics (i.e., contextual analysis or situation analysis), 2) setting objectives for the campaign, 3) designing strategy and tactics (e.g., the type of message, channel, and promotion mix), 4) scheduling, 5) budgeting, and 6) evaluation.

One of the above approaches is presented by Kotler (1997 p. 607-632). In addition to a systematic framework, Kotler gives practitioners concrete advice on setting up a campaign. For this reason, we adopt his approach as our process model for designing IS security awareness campaigns. The model consists of eight steps (Kotler 1997 p. 607): 1) identifying the target audience, 2) determining the communication objectives, 3) designing the message, 4) selecting the communication channels, 5) deciding the schedule and establishing the budget, 6) deciding on the promotion mix, 7) measuring the promotion's results and 8) managing the marketing communication process. Kotler's model does not give any consideration to the schedule of the campaign. This is added into the fifth step of our framework.

What follows is a detailed description of Kotler's framework and how Roger's and Kincaid's (1981) convergence model of communication influences the design process. *In the first phase,* the target audience is determined and the marketer must gain understanding of the audience's characteristics. Management should set the direction for an organizational change process (Beer & Nohria 2000). Hence, it should create the message of the campaign. An effective message should be accurately targeted. For this purpose, the management has to have knowledge about the characteristics of the

employees. This requires an initial amount of communication between management and employees. Because the characteristics of the employees (e.g., organizational roles, access to information, computer use, knowledge about IS security issues, technical skills) can vary widely, it might be necessary to segment the audience and decide the information to be targeted at each individual group. Segmenting the audience of an IS security awareness program is suggested e.g., by Peltier (2002), Telders (1991), Thomson and von Solms (1997), Vroom and von Solms (2002), Kovacich (1998), and Kovacich and Halibozek (2003).

In the second phase, the communication objectives are determined. This means deciding on the desired audience response. IS security awareness campaigns aim at persisting organization-wide behavioral changes (i.e., increasing user compliance with IS security instructions).

The third phase is designing the initial message to be presented during the campaign. Existing research indicates that effective information allows the recipients to form their own conclusions (cf., Kotler 1997 p. 614-615) enforcing them to active processing of the arguments presented. Furthermore, several studies (e.g., Gardner 2004, Petty & Cacioppo 1981, 1986, Chaiken, 1980, 1987) propose that the recipient's active processing of information received is necessary for permanent attitudinal and behavioral changes. Also the convergence model of communication (Rogers & Kincaid 1981) stresses that information should be actively processed but also shared (i.e., perceived, interpreted, understood, and believed) by all the communicating parties. Hence, the organization's infrastructure – both technical (e.g., applications for communication) and non-technical (e.g., organizational structures and processes) – should support sharing and collaborative processing of information in order to increase mutual understanding.

In global organizations, it is vital to localize the message as different countries vary in their culture. For example, in high context cultures (e.g., Japan) context is at least as important as what is actually said, whereas in low-context cultures most of the information is contained explicitly in the words (Czinkota, Ronkainen & Moffet 1996 p. 299). The study of culture has led to generalizations about elements that may apply across all cultures such as verbal and nonverbal language, religion, values and attitudes, manners and customs, material elements, aesthetics, education, and social institutions (Czinkota *et al.* 1996 p. 299-312). Adapting to the varying elements of different cultures requires formal training programs, including language training, environmental briefings, cultural-orientation programs, cultural assimilation, sensitivity training on flexibility in varying situations, and field experience of varying cultural environments (Czinkota *et al.* 1996 p. 318). However – regardless of the degree of training, preparation, and managers' personal characteristics – localizing a campaign requires consultation with the local management (Czinkota *et al.* 1996 p. 318).

Moreover, the audience should be taken into account when designing the contents and structure of the initial message. For example, the order of argumentation should be considered. An effective order will depend at least on the level of the knowledge of the audience and their expected attitude towards, e.g., IS security. Presenting negative arguments works best with an audience which has a high level of knowledge about the subject matter (Kotler 1997 p. 615). Furthermore, if the audience is initially opposed to the topic, it might be best to start with the audience's own arguments and conclude with the strongest positive argument (Kotler 1997 p. 615).

The fourth phase is selecting the communication channels to be used. These can be either personal or non-personal (Kotler 1997 p. 616). Personal channels involve people communicating with each other, whereas non-personal channels carry messages without personal interaction. Personal communication channels are an obvious choice when the convergence model of communication is utilized as they govern communication between people. Personal communication channels comprise expert channels (e.g., IS security specialists) and social channels. An example of a social channel is making use of influential employees and devoting extra efforts to them (cf. Kotler 1997 p. 617, Spurling, 1995). Influential employees comprise both opinion leaders, who usually belong to the same organizational class (e.g., peers) and opinion formers who usually have some kind of authority (e.g., managers) (cf., Fill 2002 p. 39-42).

The fifth phase of an IS security campaign is deciding its schedule and establishing the budget. This should include the cost of all materials, but also the time spent on the campaign.

The purpose of *the sixth phase* is to decide on the promotion mix of the campaign. The most obvious promotional tools for IS security campaigns utilizing the conversational model of communication are personal selling (e.g., IS security lectures and presentations) and direct marketing (e.g., personal or group level discussions). According to Rogers and Kincaid (1981), the communication must be conversational, targeting mutual understanding and collective action. To achieve this end, continuous dialogue between employees' representatives and management is necessary (cf., Rogers & Kincaid, 1981).

The seventh phase aims to measure the results of the campaign, i.e., the attitudinal and behavioral impact on the target audience. The research data concerning the attitudinal impact might include information on whether users recognize the message of the campaign, what points they recall, how they feel about the message, and their previous and current attitudes toward the topic of the campaign (Kotler 1997 p. 629). Behavioral response to a campaign can be evaluated, e.g., by measuring whether users follow security instructions more precisely after the campaign? Hence, in this phase the following process hypothesis (PH1) is tested.

Testable design process hypothesis for IS security awareness campaigns

PH1: It is feasible for practitioners to set up a campaign that meets MR1-MR3 and MD1 and increases user compliance with IS security instructions.

Finally, *the eighth phase* is one of managing and coordinating integrated marketing communications. This makes for a unified view of IS security issues and delivering a consistent message throughout the organization.

4.3.3 Design theory for reward and punishment

This section discusses reward and punishment as a means to improve users' IS security behavior. Rewarding users who comply with IS security instructions is an example of positive reinforcement (cf., Skinner 1991). Positive reinforcers are often understood as

tangible items – either money or exchangeable for money (Daniels 2000 p. 151). However, positive reinforcement is a wider concept as it covers the whole range of motivators that increase a certain behavior.

According to Sims and Lorenzi (1992 p. 103-108), reinforcers utilized for external influence can be classified into four major categories: (1) material, (2) symbolic, (3) social and (4) task. Potential candidates for positive material reinforcers can include such items as bonuses and salary increases whereas examples of possible punishment in this category are a cut in salary and dismissal. Symbolic and social reinforcers are not exchangeable for money. They are important for what they represent for the recipient. Potential positive reinforcers in this category include praise, recognition from peers and managers, titles, and certificates of appreciation. Example candidates for punishment related to symbolic and social reinforcement are public ridicule, harassment, and complaints. Task reinforcers are related to the work itself and include assigning more desirable tasks to the rewarded employee by means such as job rotation, new responsibilities, extended breaks, or more flexible working hours. Examples of possible punishment related to the work are closer supervision or control and inflexible working hours.

Next, kernel theories of reward and punishment in the light of reinforcement are described. In addition, the meta-requirements, meta-design and testable design product hypotheses are presented. Furthermore, the kernel theories of design process as well as the corresponding design method and testable design process hypotheses are described (Table 8).

Table 8. Design theory features for reinforcement.

Design theory features	
Design product	
Kernel theories	KT1: Skinner's theory of operant conditioning
Meta-requirements	MR1: Employees should be rewarded for complying with IS security instructions. MR2: Employees should be punished for violating IS security instructions.
Meta-design	MD1: Set an awareness program that incorporates rewards for compliance with IS security instructions. MD2: Set an awareness program that incorporates punishment for violations of IS security instructions.
Testable design product hypotheses	H1: Rewards increase compliance with IS security instructions. H2: Punishment increases compliance with IS security instructions.
Design process	
Kernel theories	KT1: Operant conditioning. KT2: The general deterrence theory
Design method	1) Taxonomy to classify IS security behaviors is designed; 2) the forms of punishment and reward are decided; 3) rewards and punishments are linked to the taxonomy of behavior; 4) it is made publicly known that IS security acts are monitored and that violators will be punished and compliers rewarded; 5) the use of punishments and rewards is implemented; and 6) the effectiveness of the use of punishment and reward is verified.
Testable design process hypothesis	It is feasible for practitioners to adopt a design process that meets MR1, MR2, MD1 and MD2 and increases users' compliance with IS security instructions.

Design product

Kernel theory of reward and punishment

Kernel Theory 1: Operant conditioning

Skinner (1991) presented the idea that manipulating environmental variables as a consequence of behavior has an impact on the recipient's behavior in the future. He found empirical evidence of functional relationships between environmental variables and the consequential behavior, and put forward the principle of operant conditioning. It is based upon the idea that learning is a function of change in behavior and that changes in behavior are the result of an individual's response to stimuli that occur in the environment. He considered any behavior acquired via reinforcement to be an example of operant conditioning. When a behavior is followed by a reward, that behavior is more likely to be repeated by the same individual in the future under similar circumstances.

Moreover, when a behavior is punished it is less likely to be repeated in the future. Hence, reinforcement is the key element of Skinner's theory of operant conditioning.

Skinner is the major proponent of operant conditioning and reinforcement. His original concepts as presented e.g., in Skinner (1991) are still accepted as the theoretical basis of reinforcement. His theory is logically reasoned and based on empirical evidence (cf., Skinner 1991). For these reasons, the theory of operant conditioning is chosen as a kernel theory of reward and punishment.

Meta-requirements for reward and punishment

Meta-requirements derived from the theory of operant conditioning (reinforcement)

MR1: Employees should be rewarded for complying with IS security instructions. According to Skinner's theory, this should increase the probability that such behavior will reoccur.

MR2: Employees should be punished for violating IS security instructions. According to Skinner's theory, this should decrease the probability that such behavior will reoccur.

Meta-design features for reward and punishment

MD1: Set an awareness program that incorporates reward and pays attention to MR1.

MD2: Set an awareness program that incorporates punishment and pays attention to MR2.

Testable design product hypotheses for reward and punishment

H1: Reward increases user compliance with IS security instructions.

H2: Punishment increases user compliance with IS security instructions.

Design process

Kernel theories of reward and punishment: reinforcement and the general deterrence theory

The theory of operant conditioning (Skinner 1991) governs the design process for reward and punishment. However, to increase the efficiency of punishment, Skinner's theory can be accomplished through the general deterrence theory (cf., Blumstein *et al.* 1978). Straub (1990) provides empirical evidence on this particular theory in the field of IS security, making it a good candidate to complement the design process for punishment. The general deterrence theory maintains that punishment and threat of punishment will tend to decrease the frequency of the targeted behaviors (Blumstein *et al.* 1978). According to the theory, deterrence has two dimensions: the severity of the sanctions and the certainty of being caught (Blumstein *et al.* 1978).

Design process for reward and punishment

Next a description of the steps required to implement the principles of reinforcement and the general deterrence theory in practice is presented. *In the first step,* behavioral goals are set. Without explicitly presenting either the wanted behaviors or those that should be avoided, it is practically impossible to punish or reward appropriately. However, it might be difficult to define all possible behaviors (IS security acts) beforehand. Rather, a set of principles (i.e., taxonomy) to classify IS security behaviors should be defined. This classification should stem from the organization's IS security policies and instructions.

In the second step, appropriate forms of reinforcement – i.e., reward and punishment – are decided. The functional definition of reward and punishment arises from the actual effect on behavior (Sims & Lorenzi 1992 p. 109). Rewards should increase compliance with and punishment decrease violations of IS security instructions.

It should be remembered that effective forms of reinforcement are personal. What reinforces someone may not work for someone else. Hence, successful outcomes depend on employees' preferences (Sims & Lorenzi 1992, Daniels 2000, Meyer 1994, Estes 1972) and managers need a basic understanding of how specific consequences might influence specific individuals. Effective use of reinforcement requires that this information is gathered from the employees (Sims & Lorenzi 1992).

There are a number of studies that give consideration to the use of performance-based incentive plans as part of organizational improvement efforts. Even though such incentives are widely used in practice, opinions on their effectiveness vary. There are studies showing that incentives influence employees' performance positively (Liska & Snell 1992, Petty, Singleton & Connell 1992). However, some studies find that employees seem to be more motivated by recognition than by money (Stuart 1992). There are also studies to show that companies have replaced cash awards with other incentives such as banquets or certificates for quality recognition (Bradt 1991, Smith 1989, Troy 1993, Wagel 1990). Furthermore, some studies argue that financial incentives are useless and may undermine intrinsic motivation (Hertzberg 2003, Kohn 1993).

Furthermore, as Festinger and Carlsmith (1959) noticed several decades ago, small monetary rewards can enhance cognitive processing among the rewarded individuals and in this way impact permanently on their attitudes. Cognitive processing is enforced by the dissonance between the recipients' attitudes and behavior (Festinger & Carlsmith 1959). According to Festinger and Carlsmith (1959), this dissonance stems from the fact that a rewarded user can not justify his behavior with the respect to magnitude of the reward. Dissonance creates tension and according to Festinger (1957), the recipient seeks tension reduction by changing his evaluations through cognitive processing. In this way, a rewarded user may change his attitude in the direction of greater compliance with IS security policies and instructions. Hence, small rewards are worth considering when persistent behavioral changes are sought through rewarding.

Moreover, Festinger and Carlsmith (1959) provide empirical evidence that significant rewards do not necessarily produce the above-mentioned attitudinal change. This result is explained by the fact that large rewards can provide a justification for taking a position contrary to one's prior attitude. Therefore, a certain behavior reinforced with large rewards does not create dissonance between the recipient's attitudes and behavior, even though his behavior is not in line with his attitudes (Festinger & Carlsmith 1959).

There are studies positing that punishment is efficient if there is a need to stop a certain behavior quickly (Azrin & Holz 1966, Corte, Wolf & Locke 1971). In addition, some studies argue that when used sparingly, punishment is effective in conveying information with respect to appropriate and inappropriate behaviors in given situations (Azrin & Holz 1966, Walters & Grusec 1977). However, the effectiveness of punishment seems to be short-lived (Driscoll 1997). In addition, punishment has side effects, which have been presented, for example, by Azrin and Holz (1966), Azrin (1967), Seligman and Maier (1967), and Sims and Lorenzi (1992) including, e.g., fear of the punishing manager, reduced communication with the manager, escape behavior (e.g., avoidance of risk), aggressive behavior, anger, and learned helplessness. Hence, albeit punishment is proven to be efficient in the context of IS security (cf., Straub 1990), the impact of the possible negative side effects should be considered.

In the third step, rewards and punishments are linked to the taxonomy of behaviors designed in the first phase. The result governs the forms of behavior that should be punished and rewarded and the corresponding consequences to the actor. However, it is impossible to define all possible behaviors in advance. Hence, instead of a comprehensive list of behaviors, a set of principles covering their classification should be designed. The intentionality (good, neutral, bad) of the act as well as the required skills are possible dimensions for the classification (Stanton *et al.* 2003).

The fourth step is to make it publicly known that users' IS security behavior is monitored and that violators of IS security instructions will be punished. This requirement stems from the general deterrence theory. In the same vein, Estes (1972) proposes that people must have an expectation of being rewarded in order for reinforcement to work. By this token, it is important to present the existence of the system of rewards and how rewards can be earned.

In the fifth step, the use of reward and punishment is implemented in practice. To support the general deterrence theory, all punishments – but not necessarily the recipients – should be made publicly known. This demonstrates that violators against IS security instructions can be caught and will be punished.

Moreover, an effective system of rewards should not limit the number of rewarded users when the goal is wide-ranging organizational change (Daniels 2000 p. 151). Everyone who achieves the set goals should be rewarded.

Finally, *in the sixth step,* the effectiveness of the use of punishment and reward is verified. During this step one or both of the following design process hypotheses (PH1 and PH2) is tested.

Testable design process hypotheses for reward and punishment

PH1: It is feasible for practitioners to adopt a design process that meets MR1 and MD1 and increases user compliance with IS security instructions.

PH2: It is feasible for practitioners to adopt a design process that meets MR2 and MD2 and increases user compliance with IS security instructions.

4.4 Research agenda for scholars and implications of the three design theories for IS security practitioners

In this chapter, the following three design theories for IS security awareness approaches were constructed: (1) training, (2) campaigns, and (3) reward and punishment. Next, a research agenda for further exploration of these three design theories is outlined. Empirical exploration requires that data on the effectiveness of the constructed awareness approaches is gathered. In addition, the feasibility of their design processes must be explored.

Each of the above-mentioned design theories aims at creating a rigorous theory-based approach to change users' attitudes and behavior. To find out whether this goal is achieved the effectiveness of the new IS security awareness approach needs to be explored. This requires the existence of empirical indicators of change in attitudes and behavior.

The remainder of this chapter proposes several research questions concerning IS security awareness design theories related to (1) IS security awareness training, (2) IS security awareness campaigns, and (3) reward and punishment. In addition, suitable research approaches for exploring the questions are suggested. Finally, the implications of the three design theories for practitioners are discussed.

4.4.1 Research agenda for IS security awareness training

As argued, IS security awareness training aims to achieve persistent organization-wide behavioral improvements. To verify whether this goal is achieved, the following research questions should be explored in practice: (1) Does theory-based IS security awareness training improve employees' IS security behavior? (2) How widespread are the resulting behavioral improvements among the employees? (3) How persistent are the resulting behavioral improvements among the employees? At the same time, the feasibility of the design method should be investigated by exploring the question (4) is deployment of the method practical?

Exploring a theory-based training program that aims at changing employee behavior corresponds to a typical aim of action research: finding solutions to the concrete problems in practice (cf., Argyris, Putnam & McLain Smith 1985 p. 8-9). Action research aims at promoting simultaneously both the theoretical conceptualization and practical command of the phenomena it studies. Action research aims to help the participants of the study in theorizing their activities, examining their theories critically in the light of action, and changing their ways of working. Hence, the present study regards action research as an appropriate approach for the practical evaluation of IS security awareness training that aims to organization-wide (social) behavioral changes.

Although action research is typically considered as an interpretive research approach, positivistic empirical indicators can also be used. They include measurable indicators of users' improved security behavior such as decreased number of virus infections. However, as behavioral changes are not always easy to measure, interpretive methods to

gather research data are also applicable. One possibility is to interview users in order to find out whether training has had any impact on their motivation, attitudes, and behavior. Another method for this purpose is to use surveys utilizing a likert-scale (e.g., five-point continuum from strongly disagree to strongly agree).

As argued, the aim of IS security awareness training should be to achieve long-lasting behavioral improvements, manifested as an increased level of compliance with IS security policies and instructions. Longitudinal studies could be used periodically to verify the state of compliance by conducting a snapshot measurement, e.g., every three to six months.

4.4.2 Research agenda for IS security awareness campaigns

As with training, campaigns also aim at persisting attitudinal and behavioral improvements on the part of users towards compliance with IS security policies and instructions. Both approaches utilize persuasive communication. Training explored through the aid of action research resembles IS security campaigns deploying the convergence model of communication. Hence, the distinction between training and campaigns can be precarious. However, from the viewpoint of this dissertation there are differences between these two awareness approaches. Training is considered as a means to provide intentioned and organized opportunities for goal-directed learning through the aid of instruction. In addition to utilizing persuasive communication, it includes the teaching of the skills and knowledge needed to comply with IS security instructions. Campaigns are merely seen as a means to sell IS security to users through persuasive information sharing (e.g., interactive lectures and discussions) that lead to mutual understanding and agreement and eventually to collective action (i.e., complying with IS security instructions). However, the research questions for exploring campaigns are similar to those for exploring training. Furthermore, the research approaches and empirical indicators resemble those of training.

4.4.3 Research agenda for reward and punishment

The present study categorizes reward and punishment as behavioral approaches, as they are based on the principles of reinforcement and operant conditioning (cf., Skinner 1991). This implies the idea that changes in behavior are the result manipulating environmental variables resulting from certain behavior. In the context of this study, this means punishing violations of and rewarding compliance with IS security instructions. Due to their same theoretical background as well as the need for an appropriate balance between the use of punishment and reward (Simms & Lorenzi 1991 p. 81), these two approaches are considered together.

In the same way as other existing awareness approaches, punishment and reward should aim at persisting organization-wide behavioral changes. Hence, the following research questions should be explored in practice: (1a) Does punishment decrease (or stop) violations of the IS security policies and instructions? (1b) Does reward increase

compliance with the IS security policies and instructions? (2) How widespread are the above-mentioned behavioral improvements among the employees? (3) How persistent are the improvements among the employees? At the same time, the feasibility of the design method should be investigated by exploring (4) is deployment of the method practical?

Measuring observable behavioral changes requires positivistic empirical indicators. As argued, these include measurable indicators of increased user compliance with IS security instructions (reward) and a decrease in the number of violations of them (punishment). The aim of punishment and reward should be to achieve persisting behavioral improvement in the form of an increased level of compliance with the IS security policies and instructions. Longitudinal studies could be used to verify periodically whether the behavioral improvements are long-lasting.

4.4.4 Implications of the three design theories for practitioners

At the organizational level, effective IS security requires that employees (i.e., IS users) are aware of the IS security measures in place as well as being motivated and capable of using them. This should be manifested as user compliance with the IS security policies and instructions. To achieve this situation – users' compliance with the IS security policies and instructions – various approaches to increase their IS security awareness should be utilized. For this purpose, we proposed three theory-based approaches: (1) training, (2) campaigns, and (3) punishment and reward. These approaches give concrete guidance on how to improve users' behavior towards compliance with organizational IS security instructions.

According to the design theorizing view, the proposed approaches are assumed to have a solid theoretical background. The aim was to utilize kernel theories with empirical evidence. For practitioners, this means that the proposed approaches are more likely to be effective. In addition, the kernel theories help practitioners to understand why the proposed IS security awareness approaches are expected to work. In addition, the theories point to the possible reasons for not achieving the desired results. This can aid further development of the three awareness approaches.

5 Empirical exploration of the design theory for IS security awareness training

The empirical part of this dissertation concentrated on exploring the design theory for IS security awareness training presented in section 4.3.1. The design theories for IS security campaigns, presented in section 4.3.2 and punishment and reward, presented in section 4.3.3, were left for further research. The empirical studies were conducted within two different companies. Because security is a sensitive subject for both companies, their identities have been disguised. The first study was of a software company (henceforth referred to as SC) and the second of an information logistics company (henceforth referred to as ILC)

The rest of this chapter presents the empirical exploration of the design theory. First, 5.1 describes the action research process at SC and 5.2 presents the action research process at ILC.

5.1 Empirical exploration of the design theory for IS security awareness training at SC

5.1.1 Background and participants

SC was established in 1997. It develops applications for electronic information processing. Its 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 described in this part of the thesis was conducted with all employees of SC, seventeen people altogether and it took place over an eleven-month time period from August, 2004 to June 2005. The management of the company consisted of three persons: CEO, marketing director and sales director. All three directors were part of the company's sales team. In addition, the team included a sales manager. The company'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 company. Additionally, he was the only formally defined manager in the company and as such, responsible for decisions covering most economic and administrative issues. The technical team was independently responsible for most product development issues. Similarly, the IS security manager was responsible for security issues.

The company had invested considerably in researching and developing its products. According to the company's management, the resulting innovations should be protected. Additionally, SC's company values include protecting its customers and business partners' information. This creates requirements for the company's IS security. For these reasons, the management of SC started an IS security development program. As one result of the program, the company's IS security management system was certified according to the BS7799 standard. Consequently, an IS security policy and end-user instructions were already in place and employees had been trained in them when this study started. Hence the management of the company and the researcher could assume a high level of employee awareness of IS security issues.

However, the company's IS security manager had noticed and also been told by employees that violations of the company's email policy were common. This policy stated that all employees should assess the criticality of information in their email messages and take the necessary precautions before sending. The policy also emphasized that confidential information should be encrypted using S/MIME when sent via email. The IS security manager described the situation in the following way: *"I have noticed that employees have sent confidential information by email 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 encrypt confidential information more often."*

The company's email policy allowed occasional exceptions to the encryption rules. It was admissible to send confidential information unencrypted if the other communicating party (e.g., business partner or customer) was unable to use email encryption. According to the company's email policy, initiating this practice required a written agreement between the communicating parties. Despite the fact that the possibility to send unencrypted email was meant for exceptional occasions, the IS security manager suspected that it was the prevailing practice at least in the sales team.

As a result of these considerations, the company's IS security manager and the researcher believed that the employees used email in a way that put valuable information at risk. They saw that this situation required improvement. Consequently, SC was selected as a host organization for empirical exploration of the design theory for IS security awareness training (see section 4.3.1). The company was interesting because of the strict IS security requirements stemming from its values, business domain and from the certified IS security management system. In addition, the size of the company made it possible to interview all employees several times during the research process. This was expected to allow rich interaction between the employees and the researcher and consequently, to provide new information regarding compliance and non-compliance with IS security policies and instructions.

5.1.2 Methodological assumptions

In this action research project, each employee of SC was considered an active processor of the information he receives. Hence, he was regarded as able to decide personally whether to comply with the company's IS security instructions, such as the email policy. Additionally, this decision was thought to be affected by his social environment. It was not expected that the IS security policies and instructions would be obeyed without their reasonableness being questioned. Hence, the present study incorporated a relativist ontology (cf., Guba & Lincoln 1989 p. 86). i.e., multiple realities socially constructed by each employee were assumed. For this reason, interaction between the researcher, management, security specialists and other employees was regarded as necessary in order to create a joint construction of the prevailing situation and to design solutions for the potential problem areas. This kind of joint construction was considered necessary for achieving the aim of this study – an increased level of compliance with the company's email policy.

5.1.3 Research strategy and position of the researcher

In this action research, the researcher was not regarded as an objective, passive outsider. The company's management, IS security manager and other employees expected him to be an active participator, helping to plan and deliver the training program and evaluate its results. Consequently, the researcher became responsible for planning the IS security awareness training program. In addition, he acted as a trainer together with the IS security manager. His further responsibilities included the planning and implementation of a new IS security communication process during the second research cycle. The researcher's involvement is best described as *expert involvement*, as the researcher was regarded as an expert among the collaborators. Some of the tasks were individual, but cooperation between the researcher and the collaborators was also an essential part of the research process (cf., Baskerville & Wood-Harper 1998 p. 95).

The action research intervention at SC aimed at increasing the level of compliance with the company's email policy by finding out and helping to overcome constraints that prevented employees from complying with the policy. Another aim was to decrease the potential wide utilization of the insecure, though permitted, exceptions to the email encryption rules. As the goal was to achieve organization-wide changes in prevailing practices, it was important to get as many employees as possible involved and committed to the change process. In the existing research, action research is considered as a suitable research strategy for exploring these kinds of issues. Kemmis and Wilkinson (2002 p. 21) emphasize that participatory action research aims to help people to investigate reality in order to change it. Hence, due to the nature and goals of this study action research was selected as the research strategy.

The action research approach is typically described as a five-phase self-reflective cyclical process (Baskerville 1999): (1) diagnosing, (2) action planning, (3) action taking, (4) evaluating, and (5) specifying learning. Furthermore, Kemmis and Wilkinson state that in addition to this self-reflective spiral, participatory action research has the

following key features: (1) it is a social process, because it deliberately sets out to investigate the relationship between the realms of the individual and the social; (2) it is a participatory process, because it encourages people to examine their knowledge and interpretive categories; (3) it is practical and collaborative, because it engages people to examine the acts which link them with others in social interaction; (4) it is emancipatory as it aims to help people to unshackle themselves from irrational, unproductive, unjust and unsatisfying social structures; (5) it is critical in its aim of helping people to recover and release themselves from the constraints embedded e.g., in their model of work; and (6) it is recursive in the aim of helping people to investigate reality in order to change it, and to change reality in order to investigate it.

SC's IS security manager stated that *"I believe that the sales team members lack the technical skills to use email encryption. In addition, some employees seem to lack knowledge about the company's information classification rules. Consequently, confidential information is not always recognized. Furthermore, I believe that there are employees who do not understand the risks related to the use of email and the possible consequences of sending unencrypted confidential information by email."* On the basis of these considerations, the researcher assumed that SC's employees needed more skills and knowledge related to email encryption and information classification. Additionally, he assumed that they needed more understanding about the possible consequences for not encrypting critical information.

Training is a common means to increase people's skills and knowledge. Furthermore, training had been used successfully at SC for inculcating new practices (e.g., new business processes) to employees. Hence, the CEO, IS security manager, and researcher considered it appropriate to address the above-mentioned shortcomings.

5.1.4 Principles of information collection and analysis

Information was collected and analyzed constantly throughout the research process. Three methods were used for collecting the research data: (1) interviews, (2) survey, and (3) participatory observation. The goal of the IS security awareness training program was to increase employees' compliance with the company's email policy. For this reason, information regarding their previous skills and knowledge of secure use of email was collected. This information was necessary for planning the training and the need for it stemmed from UCIT, one of the kernel theories of the design theory for IS security awareness training (see section 4.3.1). Consequently, a survey (Appendix 1) was used at the beginning of the process for collecting information related to employees' skills and knowledge about secure use of email.

The survey contained open questions governing information classification rules, secure use of the Internet and, especially, the secure use of email. The questions were open, but detailed, aiming to explore employees' knowledge and skills regarding the issues at state. The information gathered was used to evaluate whether the employees had the necessary knowledge for complying with the email policy.

Interviews were also used to gather information governing motivational factors related to compliance with the email policy. In addition, they were used to collect the

information governing the employees' skills and knowledge related to the subject matter and to evaluate the results of the interventions. Furthermore, informal interviews were used throughout the research process to evaluate the results.

Two types of interviews were used. The participants were interviewed in normal social interactions and using formal interview techniques. The information was recorded by means of field notes. Initially, the researcher considered using audiotape to record the interviews. This seemed to be the most useful means to avoid follow-up questions and show respect for people's time. Furthermore, it would have helped to capture the information in the participants' own terms. However, despite these advantages, the use of an audio recorder was abandoned. The reason for this was to make the participants feel more comfortable and relaxed and in this way more willing to present their own opinions and perceptions. In addition, some of the interviews were conducted in informal social situations, e.g., at the company's gym, where using a recorder would have been inconvenient.

Whenever any doubts about the meaning of an interviewee's statements arose, this was verified immediately during the interview. Further verifications were done during the analysis phase whenever this was perceived necessary to avoid wrong interpretations.

According to Stinger (1999 p. 68), a major problem with interviews is that questions are easily influenced by the researcher's perceptions, perspectives, interests, and agendas. To avoid this, the researcher used an approach proposed by Spradley (1979). This approach suggests that the researcher ask questions that are relatively neutral. This is necessary in order to diminish the extent to which participants' perceptions will be governed by frameworks of meaning unintentionally imposed by the researcher.

Spradley's (1979) approach advises the researcher to start with grand tour questions that are sufficiently global to enable participants to describe their situation in their own terms. The aim is to give focus without giving direction or suggesting forms or types of responses (e.g., "Tell me about IS security in your work."). Other possible forms of global questions include questions on what is typical (e.g., "How does your group typically act with regard to email encryption?") and on specific matters (e.g., "Describe what happened last time when you sent an email to this customer?"). When the researcher wants to gain more detailed information about issues already covered, he can present a set of questions (e.g., typical or specific) that focus on concepts already presented (e.g., "You earlier mentioned that this policy is difficult to comply with"). In all phases of the interview, the researcher should take a neutral stance and write down or record the responses as accurately as possible.

Following the approach presented above, all seventeen employees of SC were interviewed several times during the process. All the interviews were recorded by using field notes. Some of the interviews were conducted with individual employees, but group interviews were also used. The information gathered was analyzed continuously and the analysis was verified with all participants. The aim was to identify the themes that emerged from the information and whether these themes supported theories concerning compliance with IS security instructions. The analysis formed the basis for developing the intervention.

Furthermore, participatory observation concerning the impacts of the intervention was conducted in normal working situations. In addition to the researcher, the company's IS security manager and other employees observed the results achieved throughout the

study. Moreover, the researcher had large amounts of written material on hand including the company's security manual, security audit reports, memos of meetings, and risk analysis reports.

5.1.5 Conducting the action research study at SC

The intervention at SC was an IS security awareness program developed utilizing the design theory for IS security awareness training (see section 4.3.1). This eleven-month action research consisted of two research cycles. In this section, this research process is described.

Research cycle 1 at SC: IS security awareness training sessions

Identifying the problems

In the first phase of the first research cycle, the nature of the problem was explored. The first aim of this phase was to investigate whether the IS security manager's presuppositions regarding the employees' insecure use of email were correct. Another goal was to gather information necessary for designing IS security awareness training. For these purposes, all 17 employees were interviewed. In addition, a survey exploring their skills and knowledge related to the secure use of email was conducted.

As mentioned above, *the first step* in identifying the problem was an anonymous survey (Appendix 1). It aimed to explore to what extent the employees were aware of the existence of IS security instructions and whether they knew where the instructions could be found. It also gathered information about whether the employees were able to apply the email policy and information classification rules in practice. Furthermore, the survey explored the importance of email in everyday business and whether acceptable and unacceptable uses of the company's email account were known. Moreover, it targeted whether employees recognized spam and other harmful email (e.g., hazardous attachments) and the risks related to them. In addition, it was examined whether the employees were aware of the existing tools to for minimizing the risks related to email (e.g., email encryption) as well as able to use them.

Ten employees answered the survey. The analysis of the answers showed that the employees were aware of the company's IS security instructions and where the instructions could be found. This knowledge was reported by nine employees. It also became evident that email was an important business tool for everyone. Consequently, insecure use of email could cause severe risks. Moreover, all the employees recognized spam and were aware of possible hazardous email attachments.

Everyone seemed to be aware of acceptable and unacceptable use of the company's email and was able to use S/MIME encryption and digital signatures. However, only five employees were aware of possible alternatives to using S/MIME when the receiving party did not have the same capability. The fact that half of the employees were unaware of this was understandable, as S/MIME was the only encryption method defined by the company's IS security instructions. Moreover, the purpose of the information classification rules was recognized, but the rules and their utilization in practice was

unclear to three employees. Afterwards, during the interviews, this was described by one of the software developers as follows*: "The information classification rules seem to be somewhat unclear. I find it difficult to decide when encryption is really required."* Also, another software developer argued that *"Some parts of the information classification rules are unclear to me."*

The second step in identifying the problem was to interview all the employees. The interviews aimed at exploring motivational factors related to compliance with the IS security instructions – especially with the email policy. In addition, the interviews were used to supplement the information collected with the survey.

When the researcher started to analyze the information collected by the interviews, employees' answers regarding their non-compliance with the company's email policy seemed to be ambiguous and as such, difficult to categorize and analyze. To this end, the researcher created a framework for classifying and understanding the answers. The framework was derived from three motivational theories: (1) the theory of reasoned action (Fishbein & Ajzen 1975), (2) the theory of planned behavior (Ajzen 1991), and (3) the technology acceptance model (Davis 1989). The framework was used to classify answers regarding employees' motivation to comply with the company's email policy.

The central factor in the theories of Fishbein and Ajzen (1975) and Ajzen (1991) is an individual's intention to behave in a certain way. It indicates an individual's readiness to perform a given behavior and it is considered to be the immediate antecedent of behavior. An intention is based on an individual's: (I) attitude toward the behavior (Ajzen 1991, Fishbein & Ajzen 1975) and (II) subjective norm (Ajzen 1991, Fishbein & Ajzen 1975). In Ajzen (1991), these two factors are supplemented with (III) perceived behavioral control.

Attitude toward a behavior (I) is the degree to which an individual values the performance of the behavior positively or negatively. It is determined by behavioral beliefs that link the behavior to its outcomes. Subjective norm (II) is an individual's perceived social pressure to behave in a certain way. It is determined by normative beliefs concerning the expectations of important referents (e.g., peers and superiors). Furthermore, perceived behavioral control (III) refers to a person's perceived capability to perform a given behavior. It is determined by beliefs about the presence of factors that may facilitate or impede performance of the behavior.

The technology acceptance model (Davis 1989) has its theoretical grounding in the theory of reasoned action. It proposes that the major determinants defining the acceptance of a system are: (a) perceived usefulness and (b) perceived ease of use. Perceived usefulness (a) is the degree to which an individual believes that using a particular system would enhance his performance, whereas perceived ease of use (b) is the degree to which he believes that using that system does not need extra effort (Davis 1989 p. 320).

The framework, verified from the above-mentioned three theories, consisted of four classes: (Figure 5): (1) attitude towards compliance, (2) subjective norm, (3) perceived control, and (4) perceived usefulness and ease of use. Each answer regarding compliance with the company's email policy (and other IS security instructions) was classified into one of the four classes. This helped the researcher and the employees to understand the reasons for compliance and non-compliance with the instructions.

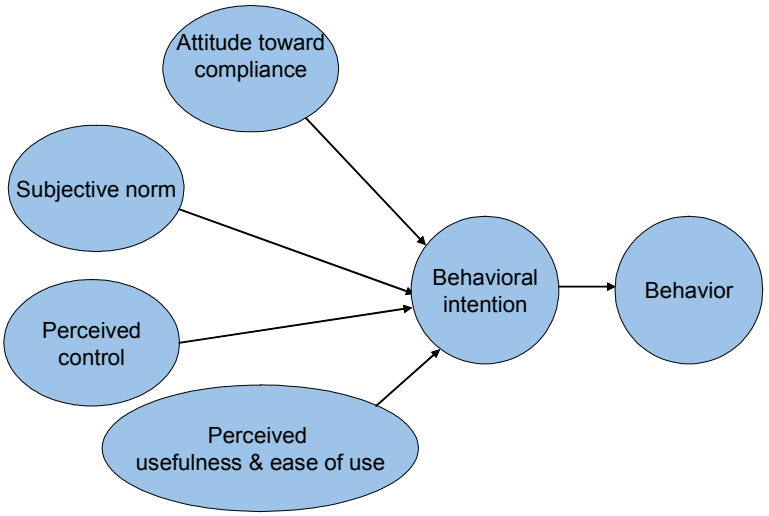

Fig. 5. Framework for analyzing employees' motivation to comply with IS security policies and instructions.

Attitude toward compliance (Figure 5)

The interviews showed that all the employees perceived good IS security as useful for the company and for one's own work. Consequently, IS security instructions and compliance with them was considered also as useful. This was illustrated, e.g., by the following comments by the employees:

Sales team member: "A high level of IS security is necessary for a company that wants to succeed in this business. Hence, our IS security instructions should be complied with whenever possible. "

Sales team member: "A high level of IS security is dictated by our company values. Otherwise it is impossible to protect our customers' sensitive information. In addition, our products must be secure. This requires that our company takes care of its security issues. Hence, we have IS security instructions and they should be complied with."

Technical specialist: "Our team, especially, processes a lot of sensitive information that must be protected. This requires compliance with the instructions. Otherwise our business could be seriously harmed. For this reason, our team considers that it is necessary to comply with the company's IS security instructions without exception."

Software developer: *"Good IS security is necessary in our business area. It is useful for the company in order to maintain its reputation. Most of the instructions are considered useful. Consequently, they are complied with by most of the employees. Our team, especially, wants to protect its innovations.* "

Subjective norm (Figure 5)

Fourteen of the employees perceived that they and their team complied with the IS security instructions in most cases. They also felt that their peers and management expected them to comply with the instructions. One of the developers described the situation in the following way: *"Because IS security is vital for us, our management takes it seriously. Hence, it aims to comply with the IS security instructions and also expects this from us."*

However, three employees argued that the instructions are not always followed by others, including management. According to them, this had an impact on their own motivation to comply with the instructions. This situation was described by one of the software developers in the following way: *"There are exceptions to compliance with the email policy. I have received unencrypted emails with confidential information from my team members, from the sales team and from management.* Furthermore, one of the technical specialists explained that *"... management seems to be busy with business issues other than security and they are too often non-compliant with the IS security instructions. This gives the sense that our management does not consider IS security important. In my opinion, this has a negative impact on employees' motivation to comply with the instructions."*

Perceived usefulness and ease of use (Figure 5)

The company's IS security instructions were considered useful and understandable. In addition, the S/MIME encryption software was considered useful and easy to use. However, four employees criticized the usefulness, clarity, accessibility, and format (MS Word document) of the security manual (including the email policy). In addition, these four employees claimed that the instructions were too bureaucratic and verbose with a lot of technical details. The latter criticism emerged most evidently in the following comments:

Software developer: *"Our security manual should be easier to access. In addition, 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 a MS Word document."*

Software developer: *"Some of the procedures in the IS security manual are complicated. In addition, they are too strict. Overall, 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. Consequently, our team members 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."*

Software that was used to protect email (i.e., S/MIME encryption) was seen as easy to use and useful for protecting valuable information. However, it was argued that sometimes the receiving party had not had the capability to use S/MIME – the only encryption method officially allowed by the company's IS security instructions.

Obviously, this had eroded the use of email encryption. One of the technicians claimed that *"…often the receiving party has no means to encrypt and decrypt emails using S/MIME. In these cases, S/MIME encryption is not useful for our purposes."*

Perceived control (Figure 5)

The interviews revealed that SC's employees recognized the contents of the company's email policy on a sufficient level. In addition, they had enough skills to use S/MIME encryption. However, four employees argued that work overload, hurry, suddenly emerging situations or unplanned assignments had been a hindrance to their compliance with the email policy. Similarly, four employees claimed that the receiver's inability to encrypt and decrypt emails was one reason for their insecure use of email.

Work overload as a reason for non-compliance with the email policy was explained by one of the technical specialists as follows: *"Sometimes the day is so busy that I simply forget instructions – including those concerning email encryption. This has happened a few times."* Work overload was also mentioned by a member of the sales team: *"The workload is occasionally so high that there is no time to even think about email encryption. In addition, there are cases when the receiving party has not been able to decrypt my email messages. Consequently, I feel that our email policy is sometimes a hindrance to a fluent business communication. I have violated the policy by sending unencrypted email."*

Furthermore, one technical specialist explained the impact of sudden, unplanned working situations on compliance with the email policy as follows: *"Sometimes management and salesmen give us strange, unplanned and urgent assignments. This makes us too busy even to think about IS security – not to mention complying with the IS security instructions."*

Conclusion of the problem analysis

The interviews revealed that the sales team did not encrypt its emails. The prevailing situation was described by a sales team member as follows: *"A lot of our team's email messages contain sensitive information. However, I suspect that about 90 percent of these emails are sent unencrypted as this is allowed by our email policy."* The IS security manager and the researcher considered the prevailing practice of sending unencrypted confidential information too risky as it jeopardized information concerning, e.g., the company's products and customers.

Furthermore, the employees argued that the company's IS security policies and instructions should be more compressed and easier to access. In addition, there had been cases when the receiving party had not had S/MIME capability. Hence, encryption was not used, which violated the email policy. Also sudden working situations (e.g., unplanned and urgent assignments given by the sales team) and work overload had caused non-compliance with the policy. Furthermore, the company's management was criticized of not showing enough of an example by arguing for IS security and complying with the company's IS security instructions.

The interviews revealed that similar problems to those with the email policy also existed with IS security procedures concerning electronic information on portable devices (e.g., USB memory sticks and CD ROMs). Four employees considered the

procedure covering taking electronic information off from SC's premises as impossible to comply with. There seemed to be two reasons for this. First, the information governing this subject was scattered around the IS security instructions. Second, the procedure for taking out electronic information from SC's premises was perceived as too complicated.

Taking out electronic information required a formal permission from a superior. This permission only covered certain types of information on certain types of devices. Hence, it was often necessary for one employee to fill in several applications: one for each type of information on each type of portable device. This process was regarded as too complicated by the employees. Consequently, information was taken out without formal permission. This situation was described by one of the software developers as follows: *"The procedure covering the removal of electronic information from our premises is difficult to find in the security manual. In addition, the procedure is far too complicated to be followed. Consequently, electronic information is taken out e.g., on USB tokens or CDs, without formal permission."* In the same vein, another software developer argued that *"The procedure covering taking electronic information off the company's premises is impossible to comply with as this would require too much time and effort."*

These considerations led the researcher and the IS security manager to consider it necessary to develop a simpler yet secure procedure to remove electronic information from the company's premises

Planning the training

The second phase of the first research cycle was planning the training sessions. The sessions were designed by the researcher with the help of the IS security manager. The planning was done through the aid of the design theory for IS security awareness training (section 4.3.1).

According to the design process (see section 4.3.1), *the first step* in the planning phase was deciding the instructional task. On the basis of the analysis performed during the previous phase of the research cycle (i.e., identifying the problem), SC's IS security manager and the researcher decided that the prevailing practice of sending confidential information unencrypted should be remedied due to the risks it caused. Consequently, the instructional task was defined as increasing the use of encryption of confidential emails. Achieving this situation – increased use of email encryption – required the learners to be aware of the existence of the email policy and its contents. In particular, they should know the rules regarding the encryption of confidential information. In addition, without sufficient knowledge of the company's information classification rules, employees would not be able to recognize confidential information. Furthermore, the employees should have the skills to use the email encryption software.

The second step in the planning phase was exploring the current situation of employees in relation to the instructional task. The difference between the knowledge that was required and the employees' current knowledge defined the learning task, i.e., what the employees still needed to learn. The employees were aware of the email policy and its contents. However, the information classification principles were unclear to three employees and hence seemed to require brushing-up.

Furthermore, the interviews indicated that the audience should be segmented as employees' technical understanding, their need to encrypt emails, and their security

behavior concerning email encryption varied. The salesmen used email in communication with SC's customers and partners, and their messages contained confidential information. Despite this, encryption was not used. The technical staff used email encryption more often. Hence, it was decided that two separate training programs with different contents would be designed: one for technical staff and one for sales and administration. Furthermore, it seemed necessary to have dedicated training sessions with the CEO in order to underline the importance of his setting an example to his employees.

Based on the above considerations, the learning task was broken down as follows. The first part of the learning task was to enable the employees to classify information according to the company's information classification rules. The second part of the learning task was to achieve employees' understanding of the importance of encrypting confidential information. Hence, the training sessions for sales and administration, in particular, should clarify the threats of sending confidential information unencrypted. Furthermore, as the use of S/MIME encryption was often impossible, the third part of the learning task was to find out about and practice alternate methods of encrypting emails.

The third step of the planning phase was constructing the learning task and the corresponding learning environment. According to the design theory of IS security awareness training (see section 4.3.1), training should (1) *take the learner's previous knowledge into account, (2) take possibilities and constraints caused by the instructional task, the learning environment, and the organizational setting into account,* (3) *enable systematic cognitive processing of information, and (4) motivate the learners for the systematic cognitive processing of information.*

The employees were segmented to two separate target groups on the basis of their previous knowledge on the topic and their current use of email encryption. As the aim was to construct training sessions that utilized the learners' existing knowledge, issues that they were already familiar with were not to be taught.

The heuristic approach described below was used to help to overcome situated constraints and utilize situated possibilities regarding the topic. In this approach, the components and functions of UCIT were combined in a matrix (Table 6). As the learner's acquisition of new knowledge formed the core of the instruction, the analysis founded on the possibilities and constraints related to it. Examples of these possibilities and constraints are given in Table 9.

Table 9. Possibilities for and constraints on learners' learning process.

	Learner		
	Acquisition	Storage	Use
Learner			
Acquisition			
Storage	1,2		
Use			
Learning environment			
Acquisition	7		
Storage	5		
Use			
Learning task	3	6	
Frame of reference	4		

Example 1: Some employees did not comply with the email encryption rules as they considered their own ways of acting better than those presented in the email policy. This was assumed to disturb their acquisition of new knowledge related to compliance with the policy. However, these employees also seemed to think actively about IS security issues. This was regarded as a possibility that should be capitalized on by employing training methods that would enhance the tendency of this group of learners to critical thinking. In addition, the intention was to emphasize the possible consequences of not complying with the email policy.

Example 2: Some employees took advantage of the permitted exceptions to the encryption rules to the point that it was as their dominant practice; this was expected to disturb their acquisition of new knowledge regarding the more secure use of email. This particular constraint was to be addressed by underlining the possible consequences of not encrypting sensitive information.

Example 3: Some employees considered compliance with the email policy harmful to communication with partners and customers. Some of them claimed that, as it was complicated to decrypt, encrypted email decreased customer and partner satisfaction. This was expected to be a constraint on the learners' acquisition of new knowledge. This was to be addressed by pointing out that there are alternative, sometimes easier ways to encrypt emails.

Example 4: Perceived lack of support by the management was expected to be a potential constraint on employees' acquisition of new knowledge. However, it was assumed the management was also interested in IS security issues. Hence, this could also provide a learning possibility. The training program aimed to activate management to promote IS security by stressing that compliance was expected of employees.

Example 5: The trainers were familiar wit IS security issues. This was recognized as a constraint if it led to the use of professional jargon instead of talking to the learner on their own terms. However, the trainers' knowledge about IS security was also a learning possibility. The goal was to avoid lecturing and instead use methods that would make the learners work actively.

Example 6: Potentially over-long lessons were considered a constraint on learners' storage of new knowledge. However, the plan was to divide the learning task into shorter parts and keep the training sessions concise. This was expected to help the learners to analyze the subject matter and memorize it.

Example 7: Trainer who would not be open to feedback from the learners was considered a constraint on learners' acquisition of new knowledge. However, openness to feedback and developing training in accordance with it was a learning possibility as it should motivate the learners. For this reason, the plan was to gather feedback throughout the training program and adjust the training sessions accordingly.

Plan for the first session: *The first IS security awareness training session* was planned to have three parts (Appendix 2). *The first part* was designed as a collaborative, instructor-led discussion concerning the threats related to the use of email. The aim was to activate the learners' existing knowledge about the subject matter. The contents of the discussion were expected to vary between the two target groups. It was assumed that the technical staff would show greater interest in technical details.

The second part was planned to deal with documents that were sent to partners and customers using email. The goal was to use the learners' own authentic documents. This

aimed to make the instruction personally relevant to the learners' and in this way to motivate their cognitive processing. According to the plan, the learner's first task was to analyze their documents and find valuable, sensitive information in them. The next task was to analyze possible consequences to the company, to the team, and to the learners themselves if such information was revealed, e.g., to competitors. The goal was to make the subject matter significant to the self and others, which in turn should motivate learners' cognitive processing. Furthermore, the purpose of the task was to building a cause-and-effect mental model to enhance long-lasting learning. Finally, instant feedback by the instructor was to be given to support persisting learning results.

The third part of the first session was planned to cover alternative ways to encrypt emails when S/MIME could not be used. It was planned as an instructor-led group discussion with the aim of finding alternative encryption methods for S/MIME. When the training was delivered it was agreed that an application called 7zip would be tested for this purpose. This affected the plan regarding the subsequent training sessions.

Plan for the second session: *The second IS security awareness training session* was planned to have two parts (Appendix 3). The plan was finalized by the researcher and the IS security manager after the first training session. *The first* part aimed to enable the employees to use 7zip for email encryption. When 7zip is used, the password that protects the encrypted file needs to be shared between 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 or a SMS message. As this was a new procedure in SC, the instructors expected most employees to be unfamiliar with the use of 7zip. Hence, the learning task for the first part was to achieve the knowledge and skills required to use 7zip to encrypt emails and to share a password through an alternative communication channel.

As argued above, similar problems to those concerning the secure use of email also existed with electronic information on portable devices such as USB memory sticks. Consequently, the goal of the *second part* was to agree upon a simple procedure to protect information on such devices. The IS security manager suggested 7zip as a potential means for this purpose. Consequently, the learning task for the second part was similar to the use of 7zip in email, except for password sharing, which was not needed.

Furthermore, the audience was segmented in the same way as in the first training session, and for similar reasons. In addition, the same heuristic approach was used to find out potential constraints and possibilities, which were found to be the same as those in the first training session.

Plan for the third session: In addition to the above-mentioned two training sessions, *a third session* was planned to accomplish them. The goal of the third session was to revise the issues governed in the first two: information classification principles, reasons for encrypting sensitive electronic information, the use of 7zip for file encryption, and two new IS security procedures: (1) the procedure for email encryption with 7zip and (2) the procedure concerning electronic information on portable devices. The third session was also to be used for evaluating the results of the training program. The evaluation was planned as an instructor-led group discussion with all SC's employees.

Delivering the training

The third phase of the first research cycle was delivering the training. *The first training session* was first held with the technical staff. The researcher and the IS security manager acted as the instructors. When the session started, all the learners except two arrived late and the instructors perceived the atmosphere to be somewhat hostile. As an example of the atmosphere, one software developer stated at the beginning of the session that *"I would have had more important things to do than attending lectures on IS security. In my opinion, this kind of training is of no use to me or our team."*

Despite this, session was delivered as planned. Surprisingly, the discussion concerning the threat to email was active. During the discussion, it became obvious that the technical employees were willing to protect their company's valuable information, but they lacked the means to do this in cases when S/MIME was unusable. Using the group's own email documents in the training was fruitful. The learners found a lot of confidential, valuable information that they had sent unencrypted. In addition, they became aware of the serious consequences for their team and the company if such information was revealed, e.g., to competitors. The learners jointly agreed that such consequences must be avoided.

To overcome the problems with S/MIME the IS security manager proposed that a program called as 7zip could be tested for email encryption. This was accepted by the learners. The reasons for using 7zip were the following: (1) the program was free of charge, (2) it supported strong encryption (e.g., AES256), and (3) using 7zip did not require a complicated infrastructure – unlike PKI-based S/MIME. One of the learners proposed the use of project-specific passwords. Then each project would have own 7zip-password shared by all the communicating parties at the beginning of the project, e.g., in at the kick-off meeting. Using this practice during the test period was agreed upon by all learners.

The researcher and the IS security manager acted as instructors in *the second session,* which was delivered according the plan. However, at the beginning of the session it was discovered that all the learners were able to use 7zip. Hence, it was not necessary to practice its use. Consequently, the second session started with a group discussion led by the instructors. The aim of the discussion was to explore whether it was possible to use 7zip for protecting electronic information on portable devices. This was jointly agreed as a feasible solution by all participants.

Furthermore, the discussion covered how the existing procedure concerning removing electronic information from the company's premises could be simplified. As a result, it was agreed that applying for formal permission to take information off SC's premises should not be required when the information is properly protected. Consequently, it was agreed that every time confidential information is taken out off the office – independent of the medium – it must be encrypted. Taking this practice up was agreed by the employees and the IS security manager – and in their next meeting also by the members of the IS security team.

The aforementioned two types of training sessions were also held with the sales team. The discussions were similar to those with the technical staff. However, as expected, they concentrated more on business issues than technical ones. In the discussions, the learners openly admitted that the existing instructions governing email protection were not complied with. Furthermore, a lot of confidential information that should not be revealed

to competitors was found in the team's previous emails. Consequently, the team agreed that this situation needed to be changed and the new practices designed and agreed with the technical team were also approved by the sales team. However, the team members were not able to use 7zip, and so this was demonstrated to them in the second session. However, the time was too short for adequate practice of the use of 7zip. Hence its use was practiced afterwards by sending and receiving 7zip-encrypted files with the help of the researcher and the IS security manager.

As planned, *the third session* was a short revision of the issues covered in the previous two sessions. It was also used for evaluation of the training program. The session consisted of an instructor-led introduction in which the IS security manager briefly presented the contents of the previous two sessions. The session was concluded by a group discussion led by the researcher. In the discussion, the results of the training program were evaluated.

In addition to the three training sessions, the researcher had several personal discussions with the company's CEO. The main point was the employees' perceived passiveness of management regarding IS security. The researcher encouraged the management to promote IS security and set an example by complying with the company's IS security instructions. This was expected to improve employees' subjective norm toward intention to comply with the company's email policy.

Evaluating the results

The fourth phase of the first research cycle was to evaluate the results of the training program. This was done in a group discussion during the third training session. In addition, all the employees were interviewed throughout the first cycle at least once in a formal interview, but also in informal social interactions, e.g., during lunch breaks and at the company's gym. These informal discussions proved to be a valuable source of research data as the employees were now more relaxed and willing to present their opinions.

In addition to interviews and discussions, participatory observation was used to gather information. During the eleven-month research project, the researcher spent several weeks at the host organization. During this time, he had the possibility to observe users' behavior, e.g., by checking received emails by users. In addition, the IS security manager, in particular, was continuously observing the results of the training program. He reported his observations spontaneously by email. Other employees also reported their observations, but only on request.

The IS security manager felt that the training program achieved positive results. He described the situation in the following way: *"The program achieved positive results. We found new solutions to encryption problems. In addition, employees' attitude towards IS security issues seems to be more positive that 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 email messages). This practice was agreed by all participants and it is now the practice in that project. I consider that he training program has achieved its goal."*

In addition, seven employees claimed that the training program had made them think about the consequences of sending unencrypted email. Consequently, five of them claimed that this had increased their use of email encryption. One of the software developers argued that *"…the training program has had an impact on our behavior. It has made me at least think about the consequences of my actions*." Another example of the results was given by a sales team member who claimed that *"As a result of the training program I have used email encryption for the first time."* Another member of the sales described the situation in the following way: *"Even on part of the sales team there has been an increase on the use of email encryption. 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 email. Hence, the training program achieved positive results."*

Furthermore, eleven employees argued that IS security procedures had been enhanced and the usability of the IS security manual had been improved as a result of the first research cycle. The manual was converted by the IS security manager from a MS Word document to an HTML document stored on the company's intranet. In addition, he had added an abstract at the beginning of each section (e.g., procedure, policy, or instruction) of the manual. The aim of the abstracts was to summarize the purpose and imperatives of each section and in this way make the manual easier to read and understand. The changes were described by one of the technical experts as follows: *"The new manual is quicker to access and the essential information is easier to find (than in the old manual)."* All these improvements to the IS security manual were suggested by the employees. Consequently, they seemed to be perceived as useful. In addition, ten employees argued that the new procedures were more feasible to comply with than their predecessors.

Despite the positive results, the need for further development remained. On the part of the sales team, there was still room for increased use of encryption. The team continuously took advantage of the permitted exceptions to email encryption. Furthermore, one of the sales team members felt that he was still unable to use 7zip after the training sessions. The researcher expected that solving these issues would require further training where such individuals would have the opportunity to practice their encryption skills and where they would be constantly reminded of the unwanted consequences of unencrypted email.

Finally, the interviews pointed out that the CEO was still considered too passive in promoting IS security issues. This was argued by five employees. This led both the researcher and the IS security manager to assume that there remained a lack of social pressure to comply with the IS security instructions.

Specifying learning

Developing and delivering the training program demonstrated that instructions, which are not considered as useful and/or easy-to-use are not complied with. Hence, before the training program started, the company's security manual was improved as suggested by the employees. This proved fruitful by making it easier for the employees to comply with the email policy. In addition, reacting to employees' suggestions for development seemed to motivate the employees toward the change process.

As argued above, the IS security awareness training program achieved positive results. The researcher perceived that the design theory for IS security awareness training (see section 4.3.1) proved to be useful in achieving this situation as it helped the instructors to concentrate on the constraints and possibilities that were specific to this particular company, subject matter and learners. In addition, it enabled the instructors to design training sessions that activated and motivated learners' collaborative, cognitive processing. Moreover, it enabled the subject matter to be made concrete and of consequence to the learners. This seemed to help to overcome the learners' negative presuppositions of IS security awareness training.

However, after the training program the IS security manager and two employees felt that IS security issues were still at too much distance from the company's other management and communication efforts. This situation was described by one of the software developers as follows: *"IS security is too distanced from the other business areas. In addition, dedicated IS security training sessions are not regarded as interesting."* In addition, the company's IS security manager felt that the training program would remain as a one-off effort to increase employees' IS security awareness. However, the CEO, the IS security manager and the researcher perceived that training should also be given regularly in the future.

Additionally, four employees felt that the management remained passive in promoting IS security. This demonstrated that these employees expected management to actively promote IS security. According to one of the software developer: *"Something must be done to get our CEO more involved in IS security management and communication. This is expected by the employees."*

During the first research cycle employees gave several suggestions for the development of IS security issues (e.g., enhancements to the format and contents of the IS security manual). However, the IS security manager considered that the employees would not propose enhancements and report problems without a direct request from him. Consequently, the researcher proposed that there should be a regular IS security discussion forum for gathering suggestions from the staff.

On the basis of the above-mentioned considerations, the researcher and the IS security manager were convinced that IS security awareness training at SC could be improved further. However, the first research cycle also showed that there were issues that were difficult to solve by awareness training alone. These issues included technical problems in the use of encryption, the participants' high workload, and unplanned sudden changes in the working situation.

Research cycle 2 at SC: a new IS security communication process

The aim of the second research cycle was to address the above-mentioned shortcomings through the aid of a new IS security communication process as described below.

Developing a new IS security communication process

The first phase of the second research cycle was planning a new IS security communication process. The aim of the process was to address the shortcomings that emerged during the first research cycle (i.e., IS security management was distanced from other management and communication efforts, management was passive in promoting IS

security issues, employees were passive in giving development suggestions and reporting problems, and continuous IS security awareness training was lacking).

The researcher and the IS security manager saw that these shortcomings could be addressed through the aid of a new IS security communication process. They perceived that such a process was required for the following three reasons. *First*, IS security training and other communication regarding IS security issues should become more closely integrated with the company's existing communication process. The IS security manager expected this to lower the perceived gap between IS security training and other communication efforts. *Second,* the process should activate the CEO to promote IS security issues more. This was expected to demonstrate the management's active involvement in IS security issues. *Third*, the process should make it easier for employees to make development proposals and report IS security problems.

SC had an existing communication process covering all business issues. The process was as follows. 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 project development, customer installation projects, and sales projects were covered. The researcher suggested that the meetings should also be used for communicating IS security issues to the staff. Hence, the researcher and the IS security manager designed a new IS security communication process, which is illustrated in Figure 6.

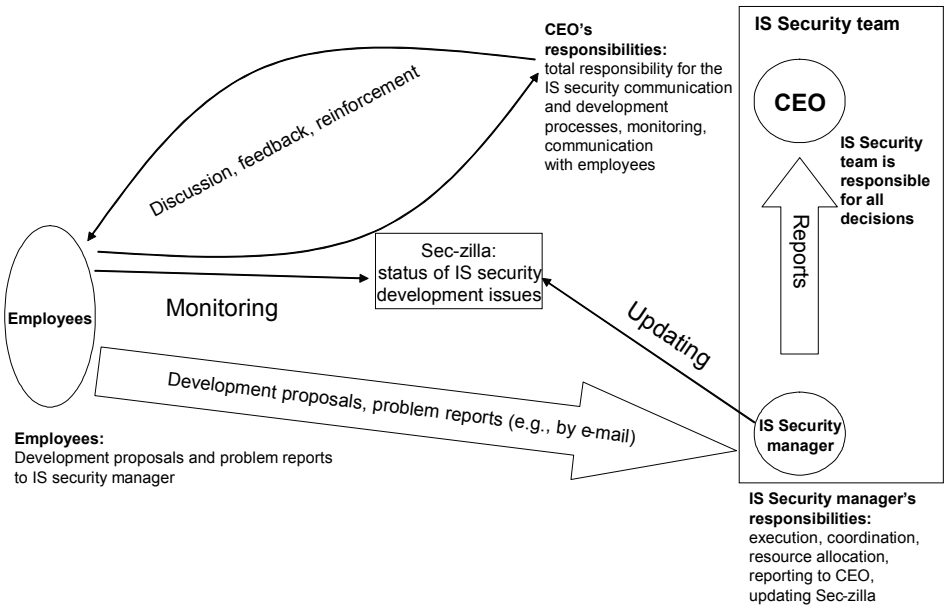

Fig. 6. SC's new IS security communication process.

In the new process, SC's IS security manager was nominated as responsible for gathering development proposals and problem reports (e.g., by email) from employees. Furthermore, it was on his responsibility to allocate resources to IS security development tasks. In addition, he was to coordinate their completion. His further responsibilities included reporting the progress of each development task to the CEO. The CEO had the overall responsibility over the process. He also became liable for active monitoring of the development tasks and communicating their progress to employees.

The new communication process was supported by a security tracking application (Figure 7). This HTML page contained information about each security task under development: reasoning, phases, progress, and the person(s) responsible for the task. This page was published in the company's intranet and it was accessible by all employees. Hence, it provided everyone with the possibility to monitor the progress of the company's IS security development tasks.

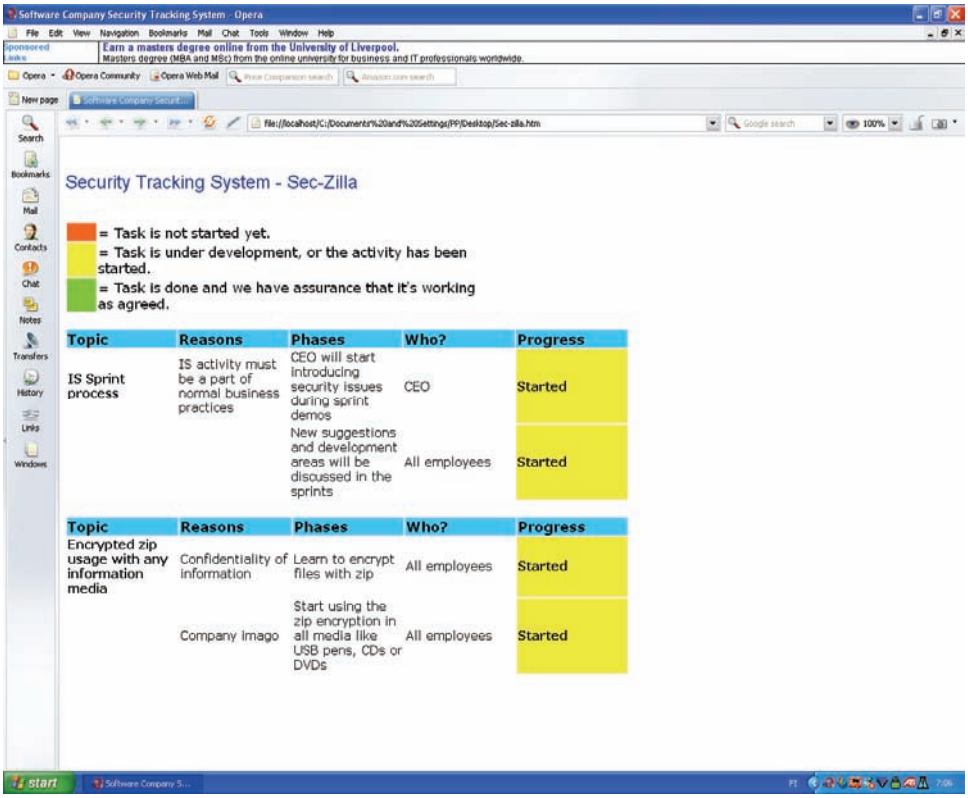

Fig. 7. An example of SC's IS security tracking system (Sec-zilla).

Implementing the new process

During the second phase of the second research cycle the new IS security development process was implemented in practice. At the beginning of the implementation phase, some problems arose. The IS security manager perceived that the CEO did not feel

comfortable presenting IS security issues to all employees. The IS security manager described the situation as follows: *"At the beginning of the session I realized that our CEO was not willing to present IS security issues to the employees. He tried to make me to do this. Finally, I managed to persuade him to present the agenda for the session, but I gave the actual presentation. His unwillingness to present IS security issues made me feel that he is not fully committed into IS security management and development."*

The employees perceived the efforts to integrate IS security communication with other business communication as worthwhile. In addition, they were not irritated by a half-hour extension to the meeting. However, the meetings did not succeed in activating the employees to discuss IS security issues. The IS security manager described this as follows: *"The staff has not been active during the sessions. They have not given any development proposals. In addition, until now only one problem has been reported. I feel that the staff may be unwilling to present their opinions freely in the CEO's presence."* Hence, the IS security manager perceived that the employees were not willing to express themselves freely in the CEO's presence. However, the employees did not confirm this during either the formal or informal discussions (interviews).

The implementation of the process encountered a serious problem when SC's IS security manager decided to leave the company and take a job as an IS security consultant. This was an obstacle to implementing the process, as he was the person in the host organization who was most actively promoting the process. In addition, collecting the research data become more difficult as the main source of participatory observation was lost.

SC's legal advisor became the new IS security manager and as such, also responsible for implementing the communication process. However, his lack of familiarity with SC's existing state of IS security was an obstacle to this. In addition, as SC's IS security management system was certified according to the BS7799 standard, there were a lot of requirements stemming from the standard. They covered, e.g., implementation of SC's risk analysis process, the need for regular IS security audits, keeping IS security policies and instructions up-to-date, and documenting all IS security acts. Consequently, the person responsible for SC's IS security would have needed a profound knowledge of the standard and its implementation in this particular company. However, the new IS security manager was quite unfamiliar with these issues. His lack of knowledge thus became another barrier for implementing the new IS security communication process. Afterwards, he described the situation in the following way: *"At the beginning, I did not feel comfortable being responsible for SC's IS security issues. I did not get any kind of introduction into IS security issues as neither the previous IS security manager nor the CEO familiarized me with the IS security manager's responsibilities. Moreover, my workload was high even without these new responsibilities."*

Owing to the inexperienced, part-time IS security manager and a passive CEO, the researcher perceived that it was going to be difficult to find someone to take responsibility for IS security management. This would stop all IS security development efforts. For this reason, the researcher decided to take an active role in promoting IS security development at SC. He helped the new IS security manager to cope with everyday IS security work, especially that related to the new IS security communication process. In addition, he tried to activate the CEO with respect to IS security management by means of persuasion.

After three months, the CEO became aware the severity of the prevailing situation. This activated him to promote IS security issues. Furthermore, as time went by, the new IS security manager became more familiar with his responsibilities. Consequently, he was able to restart IS security development efforts. As both key persons took responsibility for the monthly IS security meetings, the new communication process started to work out. However, to achieve this situation took almost five months.

Evaluating the results

Currently, the new IS security communication process is in operation. The aim is to utilize it in dealing with most of SC's IS security communication and development issues. This includes tasks such as collecting, introducing, deciding on, and prioritizing IS security development tasks and reporting their progress to employees. In addition, the IS security manager presents the results of regular audits concerning employees' security behavior.

As the above-mentioned issues are covered within the new communication process, it is expected that the need for dedicated IS security training sessions will diminish. By now, the meetings have been utilized for IS security training purposes only two times during the past five months. This seems to be too seldom as four employees asked for more regular IS security awareness training sessions. One of the software developers described the situation as follows: *"I think we need more IS security awareness training in the monthly meetings as we need continuous reminding of the existence and contents of our IS security policies and instructions."* Another software developer argued that *"In my opinion, the activity in IS security communication has been pretty low lately from both management's and employees' side. I can not remember hearing much more than monthly virus reports and the results of behavioral audits."* In addition, one of the technicians stated that *"...I have not heard anything for a while concerning IS security awareness training."* Furthermore, another software developer described the prevailing situation as follows: *"I was worried about the state of our IS security, but at the moment I am more confident as the new process has made IS security management systematic. However, the monthly meetings concentrate too much on presenting the results of the IS security audits. They should have also other contents, e.g., training."*

The researcher perceives that the new communication process has helped to achieve situation where the CEO participates in communicating SC's IS security issues to all employees. However, the IS security manager presents most of the IS security issues and the CEO is active only occasionally. This has made some of the employees feel that management is still too passive. This was described by a sales team member as follows: *"So far the management has approved all IS security development actions, but it has not been involved in IS security communication as much as probably would have been preferred."*

Furthermore, owing to the new process SC's IS security communication is integrated with other communication processes. However, according to the IS security manager, employees have not actively participated in the discussions concerning IS security matters. In addition, they have been passive about reporting IS security problems and giving suggestions for improvements. Hence, room for further development remains also in this matter.

The security tracking system, Sec-zilla, enables easy track to be kept of the progress of IS security development tasks. It helps to plan monthly meetings, as going through the changes in its IS security contents forms the core of each session. However, Sec-zilla is currently utilized for IS security management purposes only. Unlike as planned, employees are not using it to monitoring the progress of IS security development. Five employees claimed that they have revised it only during the monthly meetings. The prevailing situation was described by one of the software developers as follows: *"The new communication process and the possibility to use Sec-zilla are unclear to us. These issues have not been properly introduced by the management. This is a typical problem also in other business areas. It is not a problem that is specific to IS security management and communication."*

Specifying learning

The implementation of SC's IS security communication process showed that big organizational changes – like losing key persons – were a major hindrance to organizational development efforts. It is necessary to have an experienced, committed person responsible for IS security issues. In addition, this person needs to have visible management support in obtaining resources such as the time and the possibilities to acquire the necessary knowledge and skills to fulfill his responsibilities. Furthermore, there must be back-up arrangements for this person – as with all other key persons.

Additionally, implementing the process showed that active promotion of IS security issues by the management as well as setting an example was expected by the employees. Moreover, the implementation process underlined the fact that regular IS security awareness training was expected by the employees and that lack of training was ascribed to management's passivity in promoting IS security. Furthermore, the implementation process showed that IS security management and communication can not be separated from other management and communication efforts. Hence, generic management and communication problems emerged also in the area of IS security.

During the implementation it also became obvious that having the possibility to contribute to development efforts and monitoring their progress does not automatically guarantee active employee participation in these tasks. If these kinds of organizational practices are adopted, they must be properly introduced and clearly agreed upon. In addition, employees need constantly to be reminded of these issues.

5.1.6 Results of the intervention at SC

The action research conducted at SC consisted of two research cycles. In the first research cycle, the intervention was an IS security awareness training program designed on the basis of the design theory for IS security awareness training (see section 4.3.1). In the second research cycle, the intervention consisted of planning and implementing a new IS security communication process. Next, the results of these interventions are summarized and evaluated.

The researcher's role

During this action research study, the researcher explored the relevance, applicability and feasibility of the design theory for IS security awareness training (section 4.3.1). In addition, he took an active role in solving a practical problem experienced by the host organization: non-compliance with the email policy. The researcher was responsible for developing the IS security awareness training program during the first research cycle. His further responsibilities included acting as a trainer together with the company's IS security manager. In addition, the researcher had an active role in the company's IS security management. He was also the main force in developing the company's IS security communication process during the second research cycle.

Principles behind the training program

The IS security awareness program consisted of two training sessions with all employees and a third, brief revision session. The sessions were planned in accordance with design theorizing by utilizing the design theory for IS security awareness training (see section 4.3.1).

The training program was based on the learners' active processing of information they received. This cognitive viewpoint of learning holds that the relevant acquisition of knowledge by the learner requires him to understand the information received in a meaningful way. This understanding enables the learner to integrate new knowledge with his existing knowledge and helps long-lasting learning.

During the training sessions, learners' cognitive processing was enhanced, e.g., by the learners' collaborative efforts to extract sensitive information from their authentic, unencrypted email documents. The learners' long-lasting learning was also enhanced through a cause-and-effect mental model built by exploring the possible unwanted consequences of sending the aforementioned documents unencrypted. In addition, exploring the consequences aimed to motivate the learners to cognitive processing by making the learning task of personal relevance and of consequence for the self and others. Furthermore, such practical exercises were targeted at diminishing the learners' cognitive load.

Conclusion of the training program and its results

The IS security awareness training program achieved positive results. First, new solutions to encryption problems were found. Second, users' attitude toward IS security was improved. Third, users became more aware of the consequences of their own behavior and consequently, their use of email encryption was increased. In addition, the usability of the company's IS security manual was enhanced and some of the IS security procedures were improved.

However, the first research cycle left room for further development. The use of email encryption did not increase as desired among the sales team members. Solving this issue was expected to require further, regular training. In addition, the management was perceived as passive in promoting IS security issues and setting an example. Also employees were passive in giving suggestions for improvement and reporting problems, which again was an undesirable situation. Moreover, IS security communication was perceived too distanced from other communication efforts.

The second research cycle aimed to address the above shortcomings by means of a new IS security communication process. The process was planned so as to integrate IS security communication with other business communication efforts. In addition, it was designed to activate the CEO to regularly speak on behalf of IS security. Another target was to provide a means for continuous IS security awareness discussions and training. Moreover, the process was designed to enable the employees to propose where improvements were needed and report problems.

The new IS security communication process is now in place. The aim is to utilize the process for introducing, collecting, deciding on, and prioritizing IS security development tasks and reporting their progress to employees. Owing to the new process, SC's IS security communication is integrated with other business communication. Another achievement of the second research cycle was a new security tracking system, Sec-zilla. It was designed to help employees monitor the progress of IS security development tasks. At the moment, it is not widely used for this purpose. Furthermore, employees are still fairly passive when it comes to participating in discussions and reporting problems. Hence, there is room for further improvement. However, the researcher and the management agreed that these issues will be addressed in subsequent IS security research and development projects.

Evaluating the training program from the viewpoint of design theorizing

The goal of the action research at SC was to set a theoretically grounded and empirically validated IS security awareness program designed with the aid of the design theory for IS security awareness training (section 4.3.1). The aim was to incorporate IS security awareness training with situated learning task and environment, paying attention to the following four meta-requirements:

- *Meta-requirement 1*: IS security awareness training should take the learner's existing knowledge into account.
- *Meta-requirement 2*: IS security awareness training should take the possibilities and constraints caused by the instructional task, the learning environment, and the organizational setting into account.
- *Meta-requirement 3*: IS security awareness training should enable systematic cognitive processing of information.
- *Meta-requirement 4*: IS security awareness training should motivate systematic cognitive processing of information.

The training program addressed the aforementioned meta-requirements as follows. The *first meta-requirement* was addressed through the aid of a survey accomplished with interviews, which explored employees' knowledge on the topic. Owing to the employees' different levels of knowledge, they were segmented into two separate groups and the training was modified accordingly.

The *second meta-requirement* was addressed by analyzing the most important possibilities and constraints related to SC's employees' acquisition of new knowledge regarding this particular topic, organization and group of learners. The approach was explained in section 4.3.1.

The *third meta-requirement* was addressed in practice by learners' efforts to extract sensitive information from their authentic email documents and collaboratively exploring the possible unwanted consequences of sending those documents unencrypted. In addition, this exercise helped to address *the fourth meta-requirement* by making the learning task of personal relevance and consequence for the self and others.

In addition to addressing the above-mentioned meta-requirements, an IS security awareness training program *should increase user compliance with IS security instructions* (testable design product hypothesis, H1, section 4.3.1). As explained, this goal was reached during the research project. However, especially with the sales team, there is room for further improvement.

Finally, according to the design theorizing, it *should be feasible for practitioners to set up training that meets the four meta-requirements and increases user compliance with IS security instructions* (design process hypothesis 1, PH1, section 4.3.1). The researcher believes that this goal was met. The training program was designed according to the principles of design theorizing by utilizing the design theory for IS security awareness training and it proved to increase user compliance with IS security instructions. In addition, the design theory for IS security awareness training (section 4.3.1) proved to be useful in constructing the training program, in particular, by helping the trainers to select appropriate training methods and concentrate on the essentials regarding this particular organization, topic and group of learners.

5.2 Empirical exploration of the design theory for IS security awareness training at ILC

5.2.1 Background and participants

ILC is a subsidiary of a large Finnish corporation. Its business services include data management services, digital printing, direct marketing and electronic commerce transaction services targeted at both private and public sectors. ILC belongs into the corporation's information logistics business group. The group has 1700 employees of whom 750 are located in Finland and work at ILC. The other companies belonging into the information logistics business group are situated in Sweden, Norway, Denmark, Germany, Estonia, Latvia, and Lithuania.

The action research process described in this part of the dissertation took place over a ten-month period from January, 2005 to October, 2005. It was conducted with one of the company's business units: Data Management Services. This unit offers solutions for information managing and processing. These solutions include digitizing customers' paper documents and archiving them in electronic format, carrying out surveys, and sending large batches of marketing letters to wide audiences. The participants of the action research study were 37 employees responsible for scanning customer documents from paper into electronic form for further processing and archiving. In addition, their production manager, six production supervisors, and the business group's IS security manager participated in the research.

The business unit's production manager – along with his other duties – had the overall responsibility for the scanning process. He was assisted by six production supervisors. Their job included supporting the employees responsible for scanning the documents. The IS security manager had the overall responsibility for the business group's IS security issues.

The customers of ILC include banks, insurance companies and health care organizations. Consequently, the documents the participants process contain information about banking transactions, insurances and personal health. Protecting this kind of information is dictated by the law. In addition, such information is critical for the customers' businesses. Furthermore, protecting customers' information from unauthorized recipients and unintentional change and destruction is essential in order to maintain ILC's own and its customers' reputation.

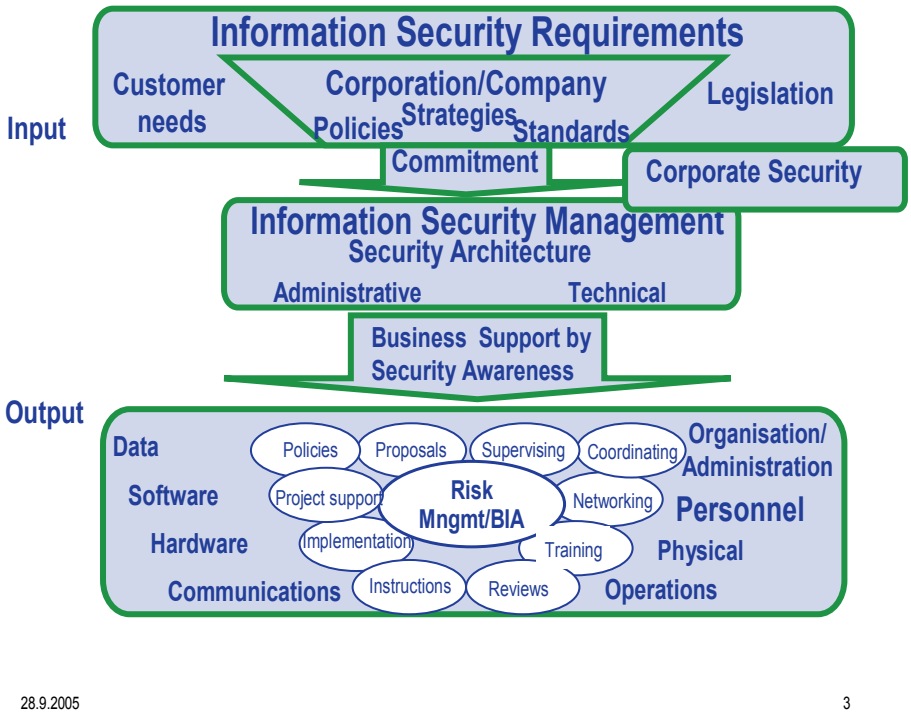

Fig. 8. IS security strategy of ILC

For the above reasons, employees' IS security awareness has a key role in ILC's IS security strategy. The strategy is illustrated in Figure 8. It emphasizes that independent of an employee's job function, he should be aware of his personal IS security mission and (optimally) committed to it.

At ILC, the employees' awareness is considered especially important as they deal with customers' information which is sensitive and critical in regard to their businesses. From the customers' viewpoint, the employees' mistakes are IS security incidents. Consequently, each mistake is potentially harmful to the customer and causes a customer complaint. It may also cause economic liabilities both to the customer and to ILC. In any case, exploring mistakes causes both the customer and ILC extra work. Moreover, mistakes erode ILC's reputation as a reliable business partner. This makes selling new services more difficult and may ultimately lead to losing customers. Hence, the production manager considered that minimizing the employees' mistakes is essential for the profitability his business. Based on the aforementioned considerations, ILC was selected as the other host organization for empirically exploring the design theory for IS security awareness training (section 4.3.1).

When this research project started, there were too many incidents per month causing customer complaints. The production manager along with the unit's production supervisors took the view that the incidents were caused – at least partly – by employees' unawareness of the fact that they are processing information critical to their customers' businesses. With these considerations in mind, the production manager proposed that an IS security awareness training program should be delivered to all employees who were responsible for the scanning process.

5.2.2 Methodological assumptions

Also in this research each participant was considered to be an active processor of the information he receives. Hence each participant was regarded as able to decide how to act when processing customers' information. This decision was considered to be affected by the social environment. Customers´ information was not expected to be protected without questioning the justification for such behavior. Hence also this action research study was based on a relativist ontology.

5.2.3 Research strategy and position of the researcher

This action research intervention aimed to make the participants more aware of the fact that they are processing information that is critical to their customers' businesses. In addition, it aimed to increase the participants' awareness of the fact that their customers' IS security is dependent on how they do their work.

As argued above, training is a common method of increasing people's skills and knowledge. Furthermore, the corporation and its subsidiary ILC, had used training for similar purposes. Consequently, the production manager, the IS security manager and the researcher saw an IS security awareness training program as a suitable way to increase employees' awareness.

As already described, creating and exploring a theory-based training program that aims at attitudinal and behavioral change corresponds to a typical aim of action research: finding solutions to concrete problems in practice (cf., Argyris *et al.* 1985 p. 8-9). Action

research aims at promoting, simultaneously, both the theoretical conceptualization and practical command of the phenomena it studies. Consequently, action research was chosen as the research strategy.

Also in this action research study, the researcher was expected to be an active participator, helping to plan and deliver the training program and evaluate its results. This was jointly agreed by the production manager, the IS security manager and the researcher. The researcher was responsible for developing the IS security awareness training program. In addition, he acted as one of the trainers together with the IS security manager and the production manager. The researcher's involvement is best described as *expert involvement* as the researcher was regarded as an expert among the collaborators. Some of the tasks were distinct, but cooperation between the researcher and his collaborators was also an essential part of the research process (Baskerville & Wood-Harper 1998 p. 95).

5.2.4 Principles of information collection and analysis

The research data was collected through interviews and surveys. An anonymous survey (Appendix 4) was used at the beginning of the process to gather data related to the production supervisors' conceptions of the role IS security in their work. The production supervisors were selected as the first group of employees from whom the research data was to be gathered. The reason for this was that the researcher and the IS security manager saw this group – complemented by the production manager – as opinion formers. In addition, they were expected to have the best insight into the prevailing situation regarding IS security in the organization. The need for this information stemmed from UCIT, one of the kernel theories of the design theory for IS security awareness training (section 4.3.1). The information was used in planning of the IS security awareness training sessions. The survey was selected as the data collection method as the workload of the production supervisors was high. For this reason, it was difficult to make an appointment for interviewing them in person. Consequently, the researcher and the IS security manager agreed that an anonymous survey was a suitable method for gathering the preliminary information which would decide the topic of the training sessions. Anonymity was chosen, because the researcher and the production supervisors were unknown to each other. For this reason, the researcher assumed that anonymity would be the best way to get authentic opinions.

At a later time, the survey was supplemented by a group interview, following the approach suggested by Spradley (1979). It aimed to find out how the production manager and the production supervisors perceived the employees' awareness regarding the nature of their work and their personal responsibility over protecting customers' information. The aim of the interviews was to find out how the opinion formers saw the prevailing situation of IS security issues in the organization. This information was used for planning the IS security awareness training sessions. For similar reasons to those presented in section 4.1, the interview was recorded using field notes.

The interview was selected as the researcher and the IS security manager saw that this would allow richer social interaction with the opinion formers. This was expected to

build mutual trust between them and the researcher. The advantages exceeded the drawbacks caused by possible problems in fitting into the participants' schedules. In addition, the production supervisors and the production manager were interviewed to verify the results of the training program. In addition, a survey (Appendix 6) was conducted with the rest of the participants (i.e., the employees) for evaluation purposes.

The anonymous survey described earlier (Appendix 4) was also used to gather data concerning employees' conceptions of IS security and its role in their work. The aim was to verify the participants' awareness regarding the nature of their work and the role of IS security in it. In addition, the goal was to explore whether the production supervisors' presuppositions regarding employees' awareness were true. This information was necessary for planning the IS security awareness training sessions. A survey was selected as there were almost 40 participants. In addition, they did not share the same working hours. As an additional barrier to personal interviews was the participants' high workload, which made it difficult to make personal appointments with them.

5.2.5 Conducting the action research study at ILC

In this section, the ten-month action research process conducted at ILC is described and evaluated. The intervention was an IS security awareness program developed utilizing the design theory for IS security awareness training (see section 4.3.1).

Identifying the problem

In the first phase, the nature of the problem was explored. T*he first step* in identifying the problem was an anonymous survey with open questions (Appendix 4). It was targeted at the production supervisors. The aim of the survey was to explore their preconceptions of IS security and its role in their work. This included how they perceive IS security and its role in their own work and in their business unit. In addition, the goal was to find out how the production supervisors see their own role and that of other employees in protecting information.

All six production supervisors answered the survey. The analysis showed that IS security was perceived as useful by everyone, especially in keeping customers satisfied and/or protecting the company's reputation. This was described by one of the supervisors as follows: *"I perceive IS security as useful for my work. Our unit is processing customers' sensitive information that must be protected from unauthorized recipients."* However, five out of the six supervisors considered IS security to be a confidentiality issue with out mentioning integrity and availability.

The analysis showed that all the supervisors regarded each employee – including themselves – as personally responsible for maintaining the company's IS security. Moreover, the researcher and the IS security manager considered the production supervisors to be influential people whose behavior had an impact on employees' attitudes toward IS security. However, no one of the supervisors spontaneously presented such a viewpoint.

The second step in identifying the problem was a group interview conducted with the production supervisors, the production manager and the business group's IS security

manager. The goal was to find out the production manager's and the production supervisors' beliefs about how the employees in this particular business unit perceive IS security. An additional aim was to explore the production manager's and supervisors' presuppositions of employees' awareness regarding the nature of their work.

The interview showed that the production supervisors regarded the employees as not fully aware of that they are processing sensitive information. One of the supervisors argued as follows: *"I suspect that many of the incidents are caused by the employees' lack of awareness. They do not recognize the value of the information they are processing*." Another production supervisor explained: *"I believe that the employees are not fully aware of the nature of their work. They consider their work as processing a pile of paper without acknowledging that they are dealing with customers' sensitive information."* Similar opinions were presented by the other supervisors and the production manager.

The third step in identifying the problem was a survey targeted at employees who were responsible for scanning the documents. The survey was the same as that used to explore the supervisors' preconceptions of IS security and its role in their work (Appendix 4). The survey was answered by 43 participants. The answers showed that IS security was seen mainly as a confidentiality issue. In addition, contrary to the expectations of the researcher and the IS security manager, employees were aware of the nature of their work and their personal responsibility for protecting customers' information. This became evident as 39 of the 43 employees answered that IS security is everyone's responsibility. Similarly, 39 employees claimed that IS security is necessary for their work as they process customers' sensitive information. For example, one of the employees argued as follows: *"I am processing documents that contain important information. It is necessary that I do not reveal this information to anyone else. I understand that our company takes IS security incidents seriously."* Another employee stated: *"I perceive that IS security plays an important role in my work, because I see a lot of sensitive information regarding organizations and individuals."*

The conclusion of the problem analysis was that IS security was seen purely as a matter of confidentiality. In addition, both the production supervisors and the employees were aware of the nature of their work and the fact that they have a role in protecting customers' sensitive information. However, the supervisors seemed not to consider that they are potential opinion formers, even though their position as influential people was taken for granted by the IS security manager and the researcher.

Planning the training

The second phase of the study was planning the training sessions. The sessions were designed by the researcher. The planning was done with the aid of the design theory for IS security awareness training (section 4.3.1).

The first step in the planning was deciding the instructional task. This was to increase employees' awareness of IS security and its role in their work. After the training program employees should be conscious that customers' IS security and business depends on their personal contribution.

The learners were divided into two separate groups: (1) the production manager and the production supervisors, and (2) other employees. This was based on the idea of the

manager and supervisors as opinion formers. Hence, an additional instructional task was to make them aware of their special position and its potential impact on IS security.

Achieving the aforementioned situation required employees to understand IS security as a matter of confidentiality, integrity and availability. In addition, it required them to be aware of the documents they processed contained customers' information, which must be protected. Furthermore, the second group (i.e., the opinion formers) should know that by their communication and exemplary behavior they might have an impact on creating a favorable attitude to protecting customers' information.

The second step in the planning phase was to explore the current state of employees knowledge related to the instructional task. The difference between the knowledge that was required and the employees' current knowledge defined the learning task, i.e., what the employees still needed to learn. As argued, the employees and the production supervisors were aware that they were processing customers' valuable information. In addition, they were aware that they were personally responsible for protecting this information. However, they considered IS security as a confidentiality issue only. Furthermore, the production supervisors were not aware of their role as opinion formers and hence, how their communication and personal example might influence on employees' motivation to protect customers' information.

On the basis of these considerations, the learning task was defined as follows. All employees were to understand that in addition to maintaining confidentiality of customers' information IS security also covers its integrity and availability. In addition, for production supervisors the learning task consisted of understanding the importance of setting an example and appropriate communication.

The heuristic approach below was used to overcome situated constraints and utilize situated possibilities regarding the subject matter. In the approach, the components and functions of UCIT were combined in a matrix (Table 10). As argued above, since the learner's acquisition of new knowledge forms the core of the instruction, the analysis concentrated on the possibilities and constraints related to it. Examples of these possibilities and constraints are given in Table 10.

Table 10. Possibilities and constraints for learners' learning process.

	Learner		
	Acquisition	Storage	Use
Learner			
Acquisition			
Storage	1		
Use			
Learning environment			
Acquisition			
Storage	4		
Use			
Learning task	2,3		
Frame of reference			

Example 1: It was expected that many employees would not have much prior knowledge about IS security. This in turn was expected to impact negatively on their acquisition of new knowledge. However, the lack of strong presuppositions could also be regarded as a possibility. The aforementioned constraint was to be overcome through the aid of an introductory e-learning package.

Example 2: It was expected that the learners would think of IS security merely as a technical matter. This was assumed to hinder the learners' acquisition of new knowledge regarding IS security as a human and organizational issue. However, this was also considered as a possibility, as the learners might regard dealing with human factors more interesting than technology.

The aforementioned constraint was to be overcome through the aid of the e-learning package, which emphasized the administrative and social aspects of IS security. In addition, the opening discussion of the training session dealt with the fact that customers' IS security is dependent on each employee's contribution.

Example 3: It was considered that the production supervisors might not be responsive to the idea of them being opinion formers. The aim was to overcome this constraint by demonstrating to them why their communication and personal example is important. This was done through the aid of the framework for analyzing employees' motivation to comply with IS security policies and instructions (Figure 5).

Example 4: Overly long lessons were considered to act as a constraint to learners' storage of new knowledge. Hence, the learning task was to be divided into shorter parts and the training sessions kept within reasonable bounds. This was expected to help the learners to analyze the subject matter and memorize it.

As stated, the target audience was segmented into two separate groups: (1) opinion formers, i.e., the production manager and the production supervisors, and (2) other employees. The training plans for these two groups were slightly different from each others.

Plans for the IS security awareness training sessions: The IS security awareness training session for the production manager and the production supervisors was planned to be given in three parts (Appendix 5). The IS security awareness training session for the rest of the employees was planned to be similar, but without the third part.

The first part was designed as an instructor-led discussion concerning IS security. The idea was to activate the learners' prior knowledge regarding the topic. In addition, the discussion aimed to show that IS security is an issue of confidentiality, integrity, and availability and dependent on employees' behavior.

The second part was planned to deal with authentic customer documents. According to the plan, the first task was to analyze these documents and find valuable information in them. The next task was to analyze the possible consequences to the company, to the business unit, and to the learners themselves if this information was destroyed, changed or revealed to unauthorized recipients. The goal was to show that – in addition to confidentiality – IS security is also a matter of integrity and availability. Additionally, the task aimed to make the subject matter significant to the self and others. This was expected to motivate the learners' cognitive processing. An additional goal was to build a cause-and-effect mental model to enhance long-lasting learning. Moreover, instant feedback from the instructor was planned to support persisting learning results.

The third part of the training session for the production manager and the production supervisors (i.e., opinion formers) was planned to cover factors influencing employees' motivation to protect customers' valuable information. The framework for analyzing employees' motivation (Figure 5) was utilized for this purpose. The aim was to emphasize that the behavior and communication of influential people has an impact on employees' subjective norm, and consequently, on achieving good IS security.

Delivering the training

The third phase was delivering the training. *The first training session* was held with the opinion formers according to the plan. The researcher and the IS security manager acted as the instructors. The discussion concerning the nature of IS security was active. Furthermore, also during this training session the learners regarded exploring authentic customer documents as fruitful. The learners found a lot of information that should be protected for unintentional change, destruction, or should not be revealed to unauthorized parties. In addition, the learners found a number of possible serious consequences to the company and business unit if this kind of information is not properly protected.

The second training session was targeted at the rest of the employees. It was planned to be held about one month after the training session for the opinion formers. However, this schedule was altered due to organizational changes. The participants' premises were moved to a new location. The old premises were situated in a compound with limited and well controlled access. However, the new premises were located in a normal residential area making unauthorized access onto the premises easier. Consequently, in addition to the schedule, also the focus of the action research project was changed.

Due to the changes in the security of the premises, the production manager and the IS security manager considered that the training efforts should be adapted accordingly. The production manager described the situation as follows: *"Due to the changes in the security of the premise, we should develop a set of rules regarding employees' behavior on the new premises and train all employees in them."* This was agreed by the production supervisors, the IS security manager and the researcher. Consequently, a set of IS security guidelines was sketched in a collaborative discussion between the production manager, the production supervisors, the IS security manager, and the researcher. It was agreed that the guidelines should concentrate on securing customers' information. In addition, they should deal with the loss of premises security caused by the new, more open environment. After the collaborative discussion, the researcher finalized the guidelines and they were agreed upon by all collaborators in a separate discussion. The IS security guidelines finalized by the researcher covered the following issues: everyone's personal responsibility over IS security, password protection, wearing identity cards and monitoring guests, handling and destroying sensitive information, and being careful with one's words off the company's premises.

The plan for the IS security awareness training session for the employees was updated as follows. The first and second parts of the session were kept as originally planned. In addition, a third part was added. It consisted of presenting the above-mentioned set of rules and connecting them to the learners' work. The third part was to be presented by the production manager. The idea behind this was to demonstrate that the managers were active in IS security issues.

In addition to changes to the contents of the session, its schedule was also changed. Due to change in business situation and the workload of the participants, the training was delayed. In this situation, the researcher perceived that no one at the host organization had the resources to follow-up the training program and its continuity seemed to be endangered. Consequently, the researcher, the IS security manager, and the production manager agreed that, in the interim, the employees would go through an e-learning package. The package was designed for IS security training across the corporation. This e-learning package covered central issues regarding IS security and it emphasized that everyone is personally responsible for IS security. The package was not targeted at any particular business unit or group of employees. Hence, it dealt with standard IS security issues in a form of a spy story. The final part of the package was an IS security test that was compulsory for every participant. Going through the package aimed to help participants to gain a basic understanding of IS security issues and, in this way, to overcome the constraints caused by a lack of prior knowledge about IS security (see Table 10).

After a delay of three months, the employees' IS security awareness training session was held with 37 participants according to the plan. The opening discussion aimed to activate the learners' existing knowledge regarding IS security. In addition, the discussion aimed to show that IS security is an issue of confidentiality, integrity and availability and is dependent on employees' behavior. At the beginning, an active discussion was not generated. However, when the discussion shifted to the contents of the e-learning package, it livened up considerably. Half of the learners considered that the package provided useful information about IS security.

The next task was exploring authentic customer documents. This was done in group discussions of four to six learners. Also in this training phase, using authentic, work-related documents proved to be fruitful. The participants were active and succeeded in finding a lot of sensitive data that must be protected. In addition, they found plenty of severe consequences to the customers, to the company and to the business unit if the aforementioned information was unintentionally changed, destroyed, or revealed to unauthorized parties.

The last part of the session covered the new IS security guidelines dealing with protecting customers' information. The presentation was given by the production manager as this was expected to demonstrate that the managers were active in IS security issues. This was thought to have a positive impact on the employees' motivation. In addition to the guidelines, the production manager presented concrete examples of how the guidelines connected directly with the learners' work e.g. by presenting issues regarding the passage control system and the destruction of work-related documents.

Evaluating the results

The training program was evaluated through the aid of an anonymous survey (Appendix 6). The survey aimed to explore how the participants perceived the e-learning package and the training session, especially from the viewpoint of their own work. It was answered by 15 of the 37 participants. In addition to the survey, the six opinion formers were interviewed in a group interview. The interview was utilized to evaluate the training session as well as the e-learning package from the standpoint of the opinion formers.

Evaluation of the e-learning package: Both the survey and the interview showed that the e-learning package was perceived as educating by the opinion formers and the other employees. This was reported by 10 participants, whereas only three perceived the package as useless for their purposes. One of the employees evaluated the package as follows: *"The package was useful for me. Especially its concrete examples regarding IS security threats were informative and increased my knowledge about information security."* Another employee argued that *"The package enabled me to learn new perspectives on information security. However, I did not consider it directly useful for my work."* Another participant reported: *"The e-learning package was educating and I learned new issues regarding IS security. However, the test was too easy."* Similar opinions were presented by another employee by arguing as follows: *"The e-learning package was accurate. I learned new perspectives on information security. However, the test was too easy."* Thus, the e-learning package seemed to have achieved its goal, which was to increase the participants' overall understanding of IS security.

Evaluation of the training sessions: The six opinion formers perceived that their training session was useful for their work. The discussion regarding protecting customers' information through the aid of authentic documents especially was seen as fruitful. The participants argued that collaborative thinking increased their awareness of IS security threats related to their daily work. In addition, they agreed that they should constantly monitor their own and employees' compliance with the behavioral rules. In addition, they committed themselves to giving feedback, both positive and negative, regarding employees' compliance with the rules. Hence, the training for the opinion formers achieved its goal.

The employees' training session was also evaluated as relevant and useful for the learners' work by eight of the fifteen employees who answered the survey. One participant evaluated the relevance of the training from the viewpoint of his work as follows: *"The training session was relevant for my work. However, I would have preferred several training sessions as the subject matter was interesting and broad."* Another employee reposted:"*...the training session was interesting and important for my work."* Furthermore, one of the learners stated: *"I consider the subject matter and the training session important and useful for my work."*

However, three employees also presented critical opinions. The criticism did not deal with the instructors, training methods, or the relevance of the subject matter. Rather, it was leveled the contents of the training session in proportion to their previous knowledge of the topic. One of these learners reposted: "*…I consider myself highly aware of IS security issues. Hence, the training was not useful for me… However, I consider that many employees learned a lot about information security and its role in our work."* Similarly, another learner presented the following criticism: *"I knew the subject matter very well already before the training, so nothing new came up."*

Additionally, eight participants argued that the training session had had an impact on their thoughts about the role of IS security's in their work. In addition, seven employees claimed that the training session had affected on their work-related behavior. Four participants reposted that there should be regular subsequent efforts to increase their IS security awareness. This was described by one of them as follows: *"This kind of training should be offered to us more often. Continuous repetition is necessary in order to have permanent results."* Furthermore, one learner stated: *"Due to the training, I understand*

better the importance and meaning of information security in my work. This has made me more careful in what I say." Similarly, another participant stated: *"I am more careful what I talk about. In addition, I monitor visitors more carefully."* Moreover, one of the learners brought up the issue that *"…information security is a larger subject than I thought and I am now more careful in my work. Before the training I did not consider that taking care of customers' documents was actually an information security issue, now I understand it."*

In addition, five participants explicitly argued that the group discussion dealing with authentic documents of ILC's customers was useful as it made them think of the possible undesirable consequences of their own behavior. In addition, one of the production supervisors claimed that working in groups was more effective than working alone would have been.

Furthermore, ten participants considered the IS security guidelines presented by the production manager as good and/or useful. The guidelines were evaluated by one participant as follows: *"The guidelines are useful. We manage well with them."* Another learner stated: *"The rules are very useful and clear."* Even though the new IS security guidelines were mainly considered to be good and useful, one participant did not feel comfortable with the idea that everyone is personally responsible for monitoring visitors. He described his feelings as follows: *"I feel uncomfortable with the idea that I am personally responsible for monitoring guests and especially that I am obliged to ask unknown and unescorted persons to identify themselves and demonstrate the purpose of their presence on the premises."*

Specifying learning

The e-learning package was evaluated as useful for providing new knowledge and understanding of IS security. This was somewhat surprising as the package had not been tailored specifically to the participants' needs. Rather, it provided standard information about IS security issues. It is possible that the positive evaluations result from the participant's lack of prior knowledge about IS security. Hence, the e-learning package provided them with new knowledge and viewpoints. Consequently, in this particular case the e-learning package provided an effective means for teaching basic knowledge to a large audience.

The training sessions had an impact on the participants' thoughts and acts. Hence, it achieved its goal. However, some of the participants claimed that the change will not be permanent without regular reminders of the importance of IS security. In addition, a more detailed segmentation of the target audience might have been more efficient as some participants considered that they were already fully aware of the issues covered. Furthermore, after the training some learners still seemed to consider IS security purely as a matter of confidentiality. Hence, in addition to confidentiality, the importance of the availability and integrity of customers' information should have been emphasized more explicitly.

The learners considered collaborative processing of authentic customer documents as fruitful as it activated their thinking and provided different perspectives on the subject matter. However, one participant considered this approach unstructured, unplanned and

unclear. Hence, for some learners a more strictly controlled assignment might have been needed.

Furthermore, this action research project proved that IS security development efforts are easily impacted by changing business situations or organizational changes. During the research process two such situations arose. One was the fusion with another company's corresponding business unit and the other was moving the business unit to a new location. Both incidents delayed the IS security awareness training program significantly. In addition, the focus of the program was lost for a while. Hence, it also became evident that there must be a person who is responsible for and committed to furthering IS security and that this person must have resources to fulfill his duties.

5.2.6 Results of the intervention at ILC

In this action research setting, an IS security awareness training program was planned and delivered. The training sessions were developed according to the principles of design theorizing by utilizing the design theory for information security awareness training (section 4.3.1). In this section, the results of the intervention are summarized and evaluated.

The researcher's role

During this action research intervention, the researcher explored the relevance, applicability and feasibility of design theory for IS security awareness training (section 4.3.1). In addition, he took an active role in solving a practical problem at the host organization: increasing employees' awareness of IS security and how it is related in their work. The researcher was responsible for developing the IS security awareness training program. His further responsibilities included acting as a trainer together with the business group's IS security manager and business unit's production manager. He also developed new IS security guidelines for the host organization. All the participants were trained in these guidelines.

Principles behind the training program

The IS security awareness program consisted of a training session for the opinion formers. In addition, it consisted of an e-learning package and a training session for all other employees. The training program was based on cognitive view of learning and the learners' cognitive processing was enhanced, e.g., by their collaborative efforts to find sensitive information in authentic customer documents. Long-lasting learning was enhanced through a cause-and-effect mental model built by exploring the possible unwanted consequences of revealing sensitive information to hostile parties as well as of changing or deleting it unintentionally. Exploring the consequences aimed to motivate the learners to cognitive processing by making the learning task of personal relevance and consequential for the self and others. Furthermore, the practical exercise was aimed at diminishing the learners' cognitive load.

Conclusion of the training program and its results

The IS security awareness training program at ILC consisted of an e-learning package and two training sessions: one for the opinion formers and the other for the rest of the employees. The aim was to increase the participants' awareness of the role of IS security in their work.

To conclude, the participants evaluated the e-learning package as useful in providing an overview of IS security issues. However, some of them did not consider the issues they learned as directly applicable to their work. However, on the basis of the participants' evaluations, the goal of the package – to increase the learners' understanding of IS security – was achieved.

The training session also achieved positive results as the participant's claimed that it had had an impact on their thoughts regarding the role of IS security in their work. In addition, the participants claimed that the training affected their work-related behavior by making them more aware of the consequences of their loose talks and careless actions. Finally, new IS security guidelines were developed and agreed upon, and the employees trained in them.

Evaluating the training program from the viewpoint of design theorizing

The goal of the action research intervention at ILC was to set a theoretically grounded and empirically validated IS security awareness program designed with the aid of the design theory for IS security awareness training (section 4.3.1). The aim was to incorporate IS security awareness training in a situated learning task and environment and pay attention to the following four meta-requirements:

- *Meta-requirement 1*: IS security awareness training should take the learner's existing knowledge into account.
- *Meta-requirement 2*: IS security awareness training should take possibilities and constraints caused by the instructional task, the learning environment, and the organizational setting into account.
- *Meta-requirement 3*: IS security awareness training should enable systematic cognitive processing of information.
- *Meta-requirement 4*: IS security awareness training should motivate to systematic cognitive processing of information.

The *first meta-requirement* was addressed as follows. First, a survey targeted at the production supervisors was carried out. The aim was to explore their existing knowledge regarding the subject matter and to adjust their training accordingly. In addition, a survey exploring other employees' existing knowledge regarding the topic was carried out in order to base the training on that knowledge.

The *second meta-requirement* was addressed by analyzing the most important possibilities and constraints related to the participants' acquisition of new knowledge regarding this particular subject matter, organization and group of learners. The approach was explained in section 4.3.1.

The *third meta-requirement* was addressed through learners' efforts to find sensitive information in authentic customer documents and by collaboratively exploring possible unwanted consequences of not protecting them properly. In addition, this exercise helped

to address *the fourth meta-requirement* by making the learning task of personal relevance and consequential for the self and others.

As argued above, an IS security awareness training program *should increase users' compliance with IS security instructions* (testable design product hypothesis, H1, section 4.3.1). The aim of this particular training program was not to targeting behavioral changes directly. Rather, the aim was to make the participants more aware of IS security and how it is related to their work. Hence, hypothesis H1 was not tested through this action research setting.

Furthermore, according to the design theory for IS security awareness training (section 4.3.1), *it should be feasible for practitioners to set up training that meets the four meta-requirements and increases user compliance with IS security instructions* (design process hypothesis 1, PH1, section 4.3.1). The researcher believes that this goal was met except in the respect that users' behavior was not explored by observation. The training program was designed according to the principles of the aforementioned design theory. In addition, the program achieved its target and the design theory for IS security awareness training (section 4.3.1) proved to be useful in developing the training program.

6 Discussion

This dissertation aimed at exploring how IS user compliance with IS security policies and instruction can be improved. This process was divided into two research steps which are summarized in Table 11.

Table 11. Research steps and respective results.

Research step	Result
What approaches are proposed in the existing research to improve users' IS security behavior and what are their strengths, weaknesses and assumptions?	A better understanding of the existing IS security awareness approaches was obtained and suggestions for researchers and practitioners were put forward.
How can users' security behavior be improved in practice?	Three design theories for information security awareness were developed and empirical evidence on the use of the design theory for IS security awareness training was provided.

6.1 Findings

Research step 1: What approaches are proposed in the existing research to improve users' IS security behavior and what are their research objectives, theoretical background, research approaches, and assumptions concerning the organizational role of IS security?

In the analysis, two categories of approaches to improve users' security behavior were found: (1) cognitive approaches and (2) behavioral approaches. Cognitive approaches included persuasive communication and active participation by involving employees in the designing of IS security measures. The most common proposal for persuasive communication was IS security awareness training. Other proposals for persuasive communication were marketing campaigns and exemplary behavior by influential people. Behavioral approaches included punishment and reward.

There was a lack of a comprehensive review of the literature on IS security awareness approaches. Such analysis was considered as useful for practitioners by deepening their understanding of the available IS security awareness approaches and their strengths and

limitations. The comprehensive review of the literature resulting from executing research step 1 is also useful for the research community by creating awareness of alternative approaches and pointing out particular issues that merit future research. Consequently, the objective of this dissertation, and in particular, the first research step, was to contribute to understanding of the existing IS security awareness approaches by analyzing them from the following viewpoints: (1) organizational role of IS security, (2) research objectives, and (3) research approach and theoretical background.

In the analysis, the most common *organizational role of IS security*, evident in 44 of the analyzed 59 studies, was socio-technical. Such a viewpoint is understandable and advantageous, because – as earlier argued – IS security is dependent not only on technical solutions, but also on users' behavior. Consequently, IS security awareness approaches should take a balanced view of end-user related and technical issues.

The most common *research objectives*, found in 47 of 59 studies, were means-end oriented. This is understandable as the studies aimed at finding means to improve users' IS security behavior. Consequently, practitioners have at their disposal a wide range of proposals providing means to influence users' security behavior.

Most, i.e. 53 of the 59, existing IS security awareness approaches employed conceptual analysis as their *research approach*. Hence, the existing IS security awareness approaches did not provide empirical evidence on their practical efficiency. An exception of this was deterrence on which Straub (1990) and Straub *et al*. (1993) provided empirical evidence. In addition, most of the existing IS security awareness approaches did not make their *theoretical background* explicit. This was only done by seven of the 59 studies. However, knowledge of the theoretical background is useful as it helps both practitioners and scholars to understand why a particular IS security awareness approach is expected to have the intended impact on users' IS security behavior. In addition, the need to use appropriate theories in the IS discipline has been noted by various scholars (e.g., Walls *et al*. 1992).

Future research should address the shortcomings pointed out by the literature review. Consequently, studies that develop theory-based cognitive and behavioral IS security awareness approaches are called for. In addition, the practical efficiency of such approaches should be empirically explored. This holds for all cognitive approaches. This dissertation presented research agendas for IS security awareness training and campaigns in sections 4.4.1 and 4.4.2. In addition, in the behavioral approaches, rewards have not been explored in the context of IS security (see also Siponen 2000b p. 206); and hence studies that empirically explore their practical efficiency are welcomed. A research agenda for rewards and punishment can be found in section 4.4.3.

Research step 2: How can users' security behavior be improved in practice?

The weaknesses found in the analysis (the lack of theoretical background and empirical evidence on practical effectiveness) were tackled as follows. *First*, the IS security awareness approaches proposed in this dissertation were developed through the aid of appropriate design theories. The design theories in turn are based on (kernel) theories. Hence, they should have a solid theoretical background. *Second*, empirical evidence on the practical effectiveness of IS security awareness training was provided through two action research interventions. The interventions were utilized to test the relevance, feasibility, and applicability of the design theory for IS security awareness training (section 4.3.1) in two companies.

Action research was perceived to be a suitable research strategy for testing this design theory and adapting the resultant training program. To summarize, the action research experiences indicate that the design theory for IS security awareness training was perceived as relevant and feasible by practitioners. In addition, it was easily applied to development and delivery of a training program. It can thus be seen as valid in terms of the accepted action research criteria. Both action research interventions were generally successful.

6.2 Relevance and validity of the action research at SC

The action research at SC tested the relevance, feasibility and applicability of the design theory for IS security awareness training (section 4.3.1) in practice by testing it through an action research setting. The goal was to explore how users' security behavior could be improved through the aid of a novel, theory-based training program. Action research is known to be a suitable research strategy for initial testing and possible adjustment of an approach. Furthermore, action research aims to help the participants to investigate reality in order to change it. This was also the goal of this study: to study and achieve organization-wide changes to prevailing practices. For these reasons, action research was selected as the research strategy.

The action research intervention at SC conforms to the seven validity criteria for information systems action research presented in section 1.2 (cf., Baskerville & Wood-Harper 1998) as follows.

First, the action research intervention at SC was set in a multivariate social situation. It was conducted with all the employees of the company involving varying relationships between the participants. In addition, the research involved complex business relationships between SC and its customers and partners. These relationships created a need for an increased use of email encryption. This was necessary for protecting SC's innovations as well as customers' and partners' sensitive information.

The prevailing situation inside the company was also complex as many of the employees considered the management passive in promoting IS security issues, which made the prevailing situation at SC challenging from the viewpoint of the intervention.

Second, the observations were stored and analyzed within an interpretive frame. When the research data was gathered, the researcher conducted all the interviews by himself. This increased the relevance of the interviews as it enabled relevant data to be gathered. 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. In addition, the employees participated twice in group interviews: once when the results of the first and once when those of the second research cycle were evaluated. The interviews were stored in the form of field notes. In addition to what was said, the body language of the interviewees was also written down. The aim was to increase the reliability of the subsequent analysis by identifying issues for further verification if the researcher perceived that all relevant issues were not made explicit.

As earlier stated, informal discussions were also used to gather the research data. These discussions proved to be a valuable data resource due to their relaxed atmosphere.

The researcher also participated in five IS security team meetings and five monthly IS security briefings. Moreover, he attended an informal company get-together. All the aforementioned occasions provided a good opportunity to build trust and gather research data. As a result of establishing mutual trust, the employees had the courage to express their feelings and perceptions quite openly. This was evident in their criticism regarding e.g., the usefulness of the training presented at the beginning of the first training session. In addition, throughout the research process several employees criticized the management to taking a passive role in promoting IS security issues. The researcher saw that the employees' courage in presenting their own viewpoints increased the validity of the research data collected from them.

The researcher stored all his observations, impressions and perceptions into a research diary for subsequent analysis. In addition, the IS security manager's email reports were a valuable source of research data. These email messages were saved for subsequent analysis. Moreover, the analysis and interpretation of the motivational factors influencing employees' compliance with the email policy utilized a theory-based framework (see Figure 5) developed for this purpose by the researcher. This data and the interpretation are provided in section 5.1.5.

Third, the researcher actively worked directly with the employees of the host organization. He had the main responsibility for designing and delivering the IS security awareness training program. In addition, he designed the new IS security communication process together with the company's IS security manager. In addition, when the IS security manager left the company, the researcher actively helped the new IS security manager to cope with his duties.

Fourth, in addition to surveys, the method of data collection included participatory observation and interviews. The researcher had the possibility to spend several weeks at the company. This provided a good possibility to participatory observation. Consequently, participatory observation was done by the researcher, but also, and especially, by the company's IS security manager, who acted as the main source of observations. He reported his observations independently and regularly by email. These emails were saved for subsequent analysis. In addition, also other employees reported their observations, but only on request.

Fifth, the outcome of the research project was assessed by reference to the collaborators' views of the success of both the training program and the communication process. As stated earlier, both the IS security manager and many of the other employees reposted that the training program achieved its goal.

Sixth, the immediate problem was resolved during the study according to the evaluations made by the collaborators. The participants reposted that their understanding of the risks related to insecure use of email increased and their compliance with the email policy improved. In addition, new solutions to email encryption problems were found. Furthermore, the collaborators perceived that the new IS security communication process made the company's IS security management more systematic.

Seventh, the actions in the first research cycle, in particular, were tightly linked to the theoretical framework of the design theory for IS security awareness training (see section 4.3.1). This framework included the universal constructive instructional theory (Schott & Driscoll 1997) and the elaboration likelihood model (Petty & Cacioppo 1981, 1986). The

framework defined the requirements for the training and explained how the training led to the present favorable outcome.

The action research intervention at SC suggests that the design theory for IS security awareness training (section 4.3.1) was relevant for the employees of the company. In addition, the researcher found it feasible and easily applied to the practical design of the IS security awareness training program at SC. Furthermore, the seven validity criteria for information systems action research presented in section 1.2 were fulfilled (cf., Baskerville & Wood-Harper 1998).

6.3 Relevance and validity of the action research at ILC

The action research at ILC tested the relevance, feasibility and applicability of the design theory for IS security awareness training (section 4.3.1). This was done in practice by testing it through an action research setting. The goal of the intervention was increasing users' awareness of IS security and how it relates to their work. In the long run, this was expected to decrease the number of customer complaints regarding the quality of the participants' work. For similar reasons to those governing the study with SC, action research was also selected as the research strategy at ILC.

The action research intervention at ILC conforms to the seven validity criteria for information systems action research presented in section 1.2 (cf., Baskerville & Wood-Harper 1998) as follows.

First, the research was set in a multivariate social situation involving complex relationships between ILC and its customers. The participants were responsible for scanning customers' paper documents in electronic form for further processing and archiving. The documents contained highly sensitive information that must be well protected. In addition, the availability of the information was often vital for customers' businesses. Hence, customers' information security was directly dependent on the participants' work and all the mistakes made by participants were noticed by the customers. Consequently, each mistake led to a complaint as well as extra work to both customers and ILC. In addition, mistakes harmed customer relationships and ILC's reputation. On the basis of the aforementioned considerations, the social situation between the participants and their customers was regarded as multivariate and complex.

Second, the observations were stored and analyzed within an interpretive frame. The action research intervention at ILC was conducted with all the employees of the business unit. This increased the reliability of the results. The researcher collected the research data mainly through surveys and group interviews. All interviews were stored as field notes and the answers to surveys and interviews were analyzed within an interpretive frame. The research data and its interpretation are provided in section 5.2.5.

Due to the changing business situation (e.g., the relocation of premises and merging with another company's department) and the workload of the participants, the researcher did not have many possibilities to spend time with the participants. Consequently, much of the research data was collected by means of surveys. The researcher perceived that compared to interviews and especially to informal discussions, surveys lack the same rich social interaction with the participants as it is not possible to see, e.g., the body language

of the respondent. In addition, anonymous surveys did not allow verification of details that the researcher considered as unclear or unconvincing. Furthermore, the little time that the researcher was able to spend with the participants did not enable as trusting relationship as that with the employees of SC to be created. This might have affected the openness of the answers – especially the amount of criticism presented regarding the contents and results of the program.

The production manager and the production supervisors were interviewed twice during the research project: once during the problem analysis phase and once when the results of the program were evaluated. The researcher interviewed the opinion formers by himself. This increased the relevance of the interviews as it enabled relevant data to be gathered. The interviews were stored in the form of field notes. In addition to what was said, the body language of the interviewees was also written down. This was done to increase the reliability of the subsequent analysis by pointing out issues for further verification if the researcher perceived that not all the relevant issues had been made explicit. Furthermore, during the action research setting, the researcher stored all his observations, impressions and perceptions into a research diary for subsequent analysis.

Third, the researcher worked directly with the employees of the host organization in designing and delivering the training program. He planned the IS security awareness training program and acted as one of the teachers together with the IS security manager and the production manager. Furthermore, he developed a set of IS security guidelines, which were agreed upon by the host organization. In addition, all the participants were trained in them during the training program.

Fourth, the lack of time spent with the participants was a hindrance to the researcher's personal participatory observation. Consequently, the method of data collection included surveys and interviews, but not participatory observation. Hence, the criterion concerning the use of participatory observation was not fulfilled.

Fifth, the outcome of the research project was assessed by reference to the collaborators' views of the success of the training program. As stated earlier, the employees evaluated both the e-learning package and the training session as educational. In addition, they argued that the training session influenced their thoughts on IS security and also their IS security behavior.

Sixth, the immediate problem was resolved during the study according to the evaluations of the collaborators. They claimed that their awareness of the role of information security in their personal work had improved and that the training had had an impact on their thoughts about IS security as well as their IS security behavior.

Seventh, the actions were tightly linked to the theoretical framework (i.e., the kernel theories) of the design theory for IS security awareness training (section 4.3.1). The kernel theories defined the requirements for the training and explained how the training led to a favorable outcome.

The action research intervention at ILC suggests that the design theory for IS security awareness training (section 4.3.1) was relevant for the employees of the company. In addition, the researcher found it feasible and easily applied to the practical design of the IS security awareness training program at ILC. However, the fourth validity criterion for information systems action research – the use of participatory observation for collecting the research data – was not fulfilled (cf., Baskerville & Wood-Harper 1998).

6.4 Limitations

This thesis has several typical limitations. With respect to the analytical part (the first research step) of this dissertation, one limitation stems from the interpretive research strategy utilized. The results are based on the researcher's interpretation. Consequently, another researcher could come into different conclusions. However, the aim was to minimize this by explicitly foregrounding those parts of the analyzed studies that led to the researcher's interpretation. Another limitation of the analysis is that its viewpoint is limited as it addresses only some of the weaknesses and strengths of the analyzed studies.

Moreover, only one of the design theories developed – the design theory for IS security awareness training (section 4.3.1) – was empirically tested. The design theories for IS security awareness campaigns (section 4.3.2) and punishment and reward (section 4.3.3) were left for further research. In addition, it could be claimed that, as the design theory was tested in two cases, only very limited support for the design theory is provided.

Moreover, theory-evolution with several research cycles was used only in the action research setting at SC. Thus, given that some scholars such as Stinger (1999) and Carr and Kemmis (1986) see theory-evolution as a necessary characteristic of an action research setting, it could be claimed that this dissertation – especially the second action research intervention – did not utilize action research in its orthodox form. Nevertheless, this is not a requirement of all action research criteria or methods (Baskerville & Wood-Harper 1998).

Action research does not aim to find general or universal mechanistic-causal laws. Rather, it aims at the provision means to take systematic action to resolve specific problems in practice (Stinger 1999 p. 17), while at the same time the relevant theories are validated through successful use. Also in the action research processes described in this dissertation, the goal was to solve practical problems experienced by the host organizations and to understand them and the results achieved from the viewpoint of theory. Consequently, the results as such can not be generalized, but they are of use in the host organizations in planning and delivering subsequent IS security awareness training programs. In addition, the results are utilizable in similar organizations as a point of departure in planning IS security awareness training programs.

6.5 Main implications and future research

The contribution of the analysis of the existing IS security awareness approaches are useful for both practitioners and researchers. For practitioners, they identify the available IS security awareness approaches and point out their strengths and weaknesses. Consequently, the practitioners benefit through knowledge of what methods can be used to increase information system users' IS security awareness. In addition, the results help them to evaluate the approaches from the viewpoint of their organizations' needs. For scholars, the analysis identifies issues for further research by revealing some of the weaknesses of the existing IS security awareness approaches.

This dissertation has also suggested three novel design theories for IS security awareness (sections 4.3.1 – 4.3.3), which would help practitioners to develop their own IS security awareness approaches. In addition, the results of action research interventions in practical settings suggest that the design theory for IS security awareness training developed here provided a useful and feasible means for building a training program. Furthermore, the action research interventions – especially the one at SC – provide empirically evaluated information on obstacles to employees' compliance with IS security policies and instructions.

7 Conclusions

This dissertation consisted of two research steps. Since there is a lack of a comprehensive review of the literature of the existing IS security awareness approaches, the first step of this dissertation was to review and evaluate the state of the existing IS security awareness research. Such analysis is useful for practitioners as they do not necessarily have time to sift a large amount of literature. For scholars, such an analysis of the literature shows what areas of IS security awareness have been studied, and to where the need for future research is most crucial.

The analysis showed that only a few of the existing studies on IS security awareness are theoretically grounded. Knowledge of the underlying theoretical background would help practitioners and scholars to understand why a particular IS security awareness approach is expected to have the desired impact on users' security behavior. Therefore, it is no surprise that the need to use appropriate theories in the IS discipline in general has been noted by scholars. Moreover, the result of the analysis revealed that most of the existing IS security awareness approaches do not provide empirical evidence on their practical effectiveness.

The second step of this dissertation was to address the shortcomings detected by the analysis by developing three novel design theories for improving information system users' IS security behavior: (1) IS security awareness training, (2) IS security awareness campaigns, and (3) punishment and reward. The design theory for IS security awareness training was then tested in two practical settings using action research. While more research and practical studies are needed, the experience gained from the action research interventions in the two organizations indicate that the proposed design theory for IS security awareness training was relevant to developing training in practice. The interventions also indicate that user compliance with IS security policies and instructions is a multifaceted construct that, in addition to knowledge and skills, relates to motivation and as such, to organizational issues like management, power and politics.

References

Ajzen I (1991) The Theory of Planned Behavior. Organizational Behavior and Human decision Processes 50(2): 179-211.

Argyris C, Putnam R & McLain Smith D (1985) Action Science. Concepts, Methods and Skills for Research and Intervention. Jossey-Bass Publishers, San Francisco.

Aytes K & Connolly T (2003) A research Model for Investigating Human Behavior Related to Computer Security. Proceedings of the Ninth Americas Conference on Information Systems: 2027-2031.

Azrin NH (1967) Pain and Aggression. Psychology Today 1: 27-33.

Azrin NH & Holz WC (1966) Punishment. In: Honig, WA (ed) Operant behavior: Areas of research and application. Appleton-Century-Crofts, New York.

Banerjee D, Cronan TP & Jones TW (1998) Modeling IT Ethics: A Study in Situational Ethics. MIS Quarterly 22(1): 31-60.

Barman S (2002) Writing IS security Policies. New Riders Publishing, Indianapolis.

Baskerville R (1999) Investigating Information Systems with Action Research. Communications of the Association for Information Systems 2 (Article 19):2-30.

Baskerville R & Wood-Harper T (1996) A Critical Perspective on Action Research as a Method for Information Systems Research. Journal of Information Technology 11: 235-246.

Baskerville R & Wood-Harper T (1998) Diversity in Information Systems Action Research Methods. European Journal of Information Systems 7: 90–107.

Beatson JG (1991) Security - a personnel issue. The importance of personnel attitudes and security education. Proceedings of the Sixth IFIP International Conference on Computer Security.

Berlo DK (1960) The Process of Communication, An Introduction to Theory and Practice. Holt, Rinehart and Winston, USA.

Blumstein A, Cochen J & Nagin D (1978) Introduction. In: Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. National Academy of Sciences, Washington D.C.

Bradt JA (1991) Pay for Impact. Personnel Journal 1991(May): 76-79.

Bray TJ (2002) Security actions during reduction in workforce efforts: what to do when downsizing. Information system security 11(1): 11-15.

Carr W & Kemmis S (1986) Becoming Critical. RoutledgeFalmer, London.

Chua WF (1986) Radical Developments in Accounting Thought. The Accounting Review, LXI: 601-632.

Chaiken S (1980) Heuristic versus systematic information processing and the use of source versus message cues in persuasion. Journal of Personality and Social Psychology 39: 752-766.

Chaiken S (1987) The heuristic model of persuasion. In: Zanna MP, Olson JM & Herman CP (eds) Social influence: The Ontario Symposium 5, Erlbaum, Hillsdale, 3-39.

Clark R (2003) Building expertise, Cognitive Methods for Training and Performance Development. International Society for Performance Improvement, Washington D.C.

Corte HE, Wolf ME & Locke BJ (1971) A comparison of procedures for eliminating self-injurious behavior for retarded adolescents. Journal of Applied Behavior Analysis 5: 201-204.

Cox A, Connolly S & Currall J (2001) Raising IS security awareness in the academic setting. VINE, Issue 123: 11-16.

Czinkota MR, Ronkainen IA & Moffet MH (1996) International Business, 4th Edition. The Dryden Press, Forth Worth.

Daniels AC (2000), Bringing Out the Best in People, How to Apply the Astonishing Power of Positive Reinforcement. McGraw-Hill, USA.

Davis F (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly 13(3): 319-340.

Deci EL & Ryan RM (1985) Intrinsic Motivation and Self-determination in Human Behavior. Plenum Press, New York.

Denning DE (1999) Information Warfare and Security. ACM Press, USA.

Desman MB (2002) Building an IS security Awareness Program. Auerbach Publications, USA.

Dick W & Carey L (1996) The Systematic Design of Instruction, 4th edition. Harper Collins, New York.

Driscoll MP (2000) Psychology of Learning for Instruction. Allyn and Bacon, Needham Heights.

Estes WK (1972) Reinforcement in Human Behavior. American Scientist 60: 723-729.

Festinger L & Carlsmith JM (1959), Cognitive consequences of forced compliance. Journal of Abnormal and Social Psychology 58: 203-210.

Figueroa ME, Kincaid DL, Rani M & Lewis G (2002) Communication for Social Change: An Integrated Model for Measuring the Process and Its Outcomes. Rockefeller Foundation, New York. Cited October 1st 2003 from http://www.rockfound.org/Documents/540/socialchange.pdf

Fill C (2002) Marketing Communications, Contexts, Strategies and Applications, 3rd edition. Prentice-Hall, Harlow.

Fischhoff B, Slovic P, Lichtenstein S, Read S & Combs B (1978) How safe is safe enough: A psychometric study of attitudes toward technological risks and benefits. Policy Sciences 9: 127-152.

Fischhoff B, Slovic P & Lichtenstein S (1979) Weighing the risks: Which risks are acceptable?. Environment 21: 17-20, 32-38.

Fishbein M & Ajzen I (1975) Belief, attitude, intention, and behavior: An Introduction to Theory and Research. Addison-Wesley, Reading.

Forcht KA, Pierson JK & Bauman BM (1988), Developing awareness of computer ethics. Proceedings of the ACM SIGCPR conference on management of information systems personnel: 142-143.

Furnell SM, Gennatou M & Dowland PS (2001) Promoting security awareness and training within small organizations. 2nd AISM Workshop, Perth, Western Australia, November, 2001. Cited April 13th 2003 from http://www.cm.deakin.edu.au/mwarren/secman/pdf/15.pdf

Furnell SM, Gennatou M & Dowland PS (2002) A prototype tool for IS security awareness and training. International Journal of Logistics Information Management 15(5): 352-357.

Furnell S, Sanders PW & Warren MJ (1997) Addressing IS security training and awareness within the European healthcare community. Proceedings of Medical Informatics Europe '97.

Gagné RM (1985) The Conditions of Learning (4th ed). CBS College Publishing, New York.

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

Gaunt N (1998) Installing an appropriate IS security policy [in hospitals]. International Journal of Medical Informatics 49(1): 131-134.

Gaunt N (2000) Practical approaches to creating a security culture. International Journal of Medical Informatics 60(2): 151-157.

Glaser R (1971) The Design of Instruction. In: Merrill MD (ed) Instructional Design: Readings. Prentice-Hall, Englewood Cliffs.

Greenwald AG. (1968) Cognitive learning, cognitive response to persuasion, and attitude change. In; Greenwald AG., Brock TC & Ostrom TM (eds) Psychological foundations of attitudes. Academic Press, San Diego, 147-170.

Guba EG & Lincoln YS (1989) Fourth Generation Evaluation. Sage Publications, Newbury Park.

Habermas J (1984) The Theory of Communicative Action, Volume One; Reason and the Rationalization of Society. Beacon Press, Boston.

Hadland T (1998) IS security management - an awareness campaign. Proceedings of New Networks, Old Information: UKOLUG98, UKOLUG's 20th Birthday Conference 1998.

Hansche S (2001a) Designing a Security Awareness Program: Part I, Information system security 10(1): 14-22.

Hansche S (2001b) Information System Security Training: Making It Happen, Part 2. Information system security 10(3): 51-70.

Hare RM (1981) Moral Thinking: its levels, method and point. Oxford University Press, Oxford.

Herzberg F (2003) One More Time: How Do You Motivate Employees?. Harvard Business Review 2003 (January): 87-96.

Hevner AR March ST, Park J & Ram S (2004) Design Science in Information Systems Research. MIS Quarterly 28(1): 75-105.

Iivari J (1991) A paradigmatic analysis of contemporary schools of IS development. European Journal of Information Systems 1(4): 249-272.

Iivari J & Hirschheim R (1996) Analyzing Information Systems Development: A Comparison and Analysis of Eight Development Approaches. Information Systems 21(7): 551-575.

Iivari J & Kerola P (1983) A Sociocybernetic Framework for the Feature Analysis of Information Systems Design Methodologies. In: Olle TW, Sol HG & Tully CJ (eds) Information Systems Design Methodologies: A Feature Analysis. Elsevier Science Publishers, North-Holland, Amsterdam, 87-139.

International Organization for Standardization (ISO) (2005) ISO/IEC 17799, Information technology - Code of practice for IS security management, Second Edition.

International Security Forum (ISF) (2005) The Forum's Standard of Good Practice for IS security, January 2005. Cited March 14th 2006 from http://www.isfsecuritystandard.com/index_ie.htm.

Järvinen P (1997) The New Classification of Research Approaches. In: Zemanek H (ed) The IFIP Pink Summary - 36 years of IFIP. IFIP, Laxenburg, Austria, 124-131.

Järvinen P (2000) Research Questions Guiding Selection of an Appropriate Research Method. Proceedings of the 8th European Conference on Information Systems (ECIS 2000).

Kabay ME (2002) Using Social Psychology to Implement Security Policies. In: Bosworth S & Kabay ME (eds) Computer Security Handbook, 4th edition. John Wiley & Sons, Inc., USA, 32.1-32.16.

Kajava J & Siponen MT (1997) Effectively Implemented IS security Awareness - An Example from University Environment. Proceedings of IFIP-TC 11 (Sec'97/WG 11.1), 13th International Conference on IS security: IS security Management - The Future.

Katsikas SK (2000) Health care management and information system security: awareness, training or education?. International Journal of Medical Informatics 60(2): 129-135.

Kemmis S & Wilkinson M (1998) Participation action research and the study of practice. In: Atweh B, Kemmis S & Weeks P (eds) Action research in practice. Routledge, London, 21-36.

Kincaid DL (1979) The Convergence Model of Communication, Honolulu, East-West Communication Institute, Paper 18.

Kincaid DL (1988) The Convergence Theory of Communication: Its Implication for Intellectual Communication. In: Kim YY (ed) Theoretical Perspectives International and Intercultural Annual XII: 280-298.

Kluge EHW (1998) Fostering a security culture: a model code of ethics for health information professionals. International Journal of Medical Informatics 49(1): 105-110.

Kohlberg L (1981) The Philosophy of Moral Development. Harper and Row, San Francisco.

Kohn A (2002) Why Incentive Plans Cannot Work. HBR OnPoint, Best of HBR on Motivation: 51-57. Harvard Business School Publishing, USA.

Korschun H (1998) Study shows education cuts down risk of AIDS infection, Emory Report 50(36). Cited March 3rd 2004 from http://www.emory.edu/EMORY_REPORT/erarchive/1998/August/eraugust.3/8_3_98Contents.html.

Kotler P (1997) Marketing Management, Analysis, Planning, Implementation, and Control. Prentice Hall, Upper Saddle River.

Kotter JP & Schlesinger LA (1979) Choosing strategies for change. Harvard Business Review (March-April): 106-114.

Kovacich GL (1998) Information system security Officer's Guide: Establishing and Managing an Information Protection Program. Butterworth-Heinemann, USA.

Kovacich GL & Halibozek EP (2003) The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program. Butterworth-Heinemann, USA.

Lafleur LM (1992) Training as part of a security awareness programme. Computer Control Quarterly 10(4): 4-11.

Liska RW & Snell B (1992) Financial Incentive Programs for Average-size Construction Firms. Journal of Construction Engineering and Management 118(4): 667-676.

Markey E (1989) Getting organizations involved in computer security: the role of security awareness. Proceedings of the Fifth IFIP International Conference.

Markus ML, Majchrzak A & Gasser L (2004) A Design Theory for Systems That Support Emergent Knowledge Processes. MIS Quarterly 26(3): 179-212.

Martins A & Eloff JHP (2002) IS security Culture. Proceedings of IFIP TC-11 17th International Conference on IS security (SEC2002).

McGuire WJ (1968) Personality and attitude change: An information-processing theory. In: Greenwald AG, Brock TC & Ostrom MT (eds) Psychological foundations of attitudes: 171-196. Academic Press, San Diego.

McGuire WJ (1972) Attitude change: The information processing paradigm. In: McClintock CG (ed) Experimental social psychology. Rinehart & Winston, New York, 108-142.

McLean K (1992) IS security awareness - selling the cause. Proceedings of the IFIP TC11, 8th International Conference on IS security, IFIP/Sec '92.

Meyer P (1994) Can You Give Good, Inexpensive Rewards? Some real-life answers. Business Horizons (November-December): 84-85.

Mill JS (1987), Utilitarianism. In: Mill JS, Bentham J & Ryan A (ed) Utilitarianism and Other Essays, Penguin Books, London, 272-338.

Mitnick KD (2002) The Art of Deception: Controlling the Human Element of Security. Wiley Publishing, USA.

Murray B (1991) Running corporate and national security awareness programmes. Proceedings of the IFIP TC11 Seventh International Conference on IS security: 203-207.

National Institute of Standards and Technology (NIST) (1996) Technology Administration, U.S. department of Commerce, An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12. Cited January 13th 2006 from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

National Institute of Standards and Technology (NIST) (1998) Information Technology Security Training Requirements: A Role- and Performance-Based Model, NIST special publication 800-16. Cited January 7th 2006 from http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

National Institute of Standards and Technology (NIST) (2003) Building an Information Technology Security Awareness and Training Program, NIST special publication 800-50. Cited January 5th 2006 from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Parker DB (1998) Fighting Computer Crime: A new Framework for Protecting Information. John Wiley & Sons, USA.

Parker DB (1999) Security motivation, the mother of all controls, must precede awareness. Computer Security Journal 15(4): 15-23.

Peltier T (2000) How to build a comprehensive security awareness program. Computer Security Journal 16(2): 23-32.

Peltier T (2002) IS security Policies, Procedures, and Standards. Guidelines for Effective IS security Management. Auerbach Publications, USA.

Perry WE (1985) Management Strategies for Computer Security. Butterworth Publishers, USA.

Petty RE & Cacioppo JT (1981) Attitudes and persuasion: Classic and contemporary approaches. Brown, Dubuque.

Petty RE & Cacioppo JT (1986) The elaboration likelihood model of persuasion. In: Berkowitz L (ed) Advances in experimental social psychology 19: 123-205.

Petty MM, Singleton BB & Connell DW (1992) An Experimental Evaluation of an Organizational Incentive Plan in the Electric Utility Industry. Journal of Applied Psychology 77: 427-436.

Pipkin DL (2000) IS security: Protecting the Global Enterprise, Hewlett-Packard Professional Books. Prentice Hall PTR, Upper Saddle River, USA.

Proctor PE & Byrnes FC (2002) The Secured Enterprise: Protecting Your Information Assets. Prentice Hall, Upper Saddle River, USA.

PriceWaterhouseCoopers (2004) IS security Breaches Survey 2004. Cited February 9th 2006 from http://www.pwc.com/Extweb/service.nsf/docid/B2ECC9B0E9EFA3D785256C33005247D3.

Puhakainen P & Siponen MT (2005) Three design theories for IS security awareness. Unpublished research paper, University of Oulu.

Rawls JA (1999) A Theory of Justice, Revised Edition. Harvard University Press, Cambridge.

Rodriguez L & Anderson-Wilk M (ed) (2002) Communicating Highway-safety: What Works. Center for Transportation. Research and Education, Iowa state University. Cited May 4th 2006 from http://ntl.bts.gov/lib/22000/22800/22892/chs.pdf.

Rogers EM (1962) Diffusion of Innovation. Free Press, New York.

Rogers EM & Kincaid DL (1981) Communication Networks: Toward a New Paradigm for Research. Free Press, New York.

Rudolph K, Warshawsky G & Numkin L (2002) Security Awareness. In: Bosworth S & Kabay ME (eds) Computer Security Handbook, 4th edition. John Wiley & Sons, USA, 29.1-29.19.

Sasse A, Brostoff S & Weirich D (2001) Transforming the 'weakest link' a human / computer interaction approach to usable and effective security. BT technology journal 19(3): 122-131.

Schlienger T & Teufel S (2002) IS security Culture: The Socio-Cultural Dimension in IS security Management. Proceedings of IFIP TC 11.

Schott F & Driscoll MP (1997) On the Architectonics of Instructional Theory. In: Tennyson RD, Schott F, Seel N & Dijkstra S (eds) Instructional Design: International Perspective, Vol. 1, Theory, Research, and Models. Lawrence Erlbaum Associates, Mahwah, 135-173.

Schramm W (1954) How Communication Works. In: Schramm W (ed) The Process and Effects of Mass Communications. University of Illinois Press, Urbana.

Schramm W (1973) Men, Messages and Medium: A Look and Human Communication. Harper and Row, New York.

Seligman MEP & Maier SF (1967) Failure to escape traumatic shock. Journal of Experimental Psychology 74: 1-9.

Shannon C & Weaver W (1962) The Mathematical Theory of Communication. University of Illinois Press, Urbana.

Sims HP & Lorenzi P (1992) The New Leadership Paradigm, Social Learning and Cognition in Organizations. Sage Publications, Newbury Park.

Siponen MT (2000a) A conceptual foundation for organizational IS security awareness. Information Management & Computer Security 8(1): 31-41.

Siponen MT (2000b) Critical analysis of different approaches to minimizing user-related faults in information system security: implications for research and practice. Information Management & Computer Security 8(5): 197-209.

Siponen MT (2000c) On the Role of Human Morality in Information System Security: The Problems of Descriptivism and Non-descriptive Foundations. Proceedings of IS security for Global Information Infrastructures, IFIP TC11 Fifteenth Annual Working Conference on IS security: 401-410.

Siponen MT (2001) Five dimensions of IS security awareness. ACM SIGCAS Computers and Society 31(2): 24-29.

Skinner BF (1991) The behavior of organisms: An experimental analysis. B.F. Skinner Foundation (reprinted).

Slovic P (1987) Perception of risk. Science 236: 280-285.

Smith DC (1989) The Role of Incentives in Service Quality. Bank Marketing (October): 21-22.

Spradley JP (1979), The Ethnographic Interview. Wadsworth, Belmont.

Spurling P (1995), Promoting security awareness and commitment. Information Management & Computer Security 3(2): 20-26.

Stacey TR (1996) IS security Program Maturity Grid. Information system security 5(2): 22-33.

Stanton JM, Caldera C, Isaac, A, Stam KR & Marcinkowski SJ (2003), Behavioral IS security: Defining the criterion space. In: Mastrangelo PM & Everton WJ (eds) The Internet at work or not: Preventing computer deviance. Symposium presentation at the meeting of the society for Industrial and Organizational Psychology, Orlando.

Stinger ET (1999) Action Research, Second Edition. Sage Publications, Thousand Oaks.

Straub DW (1990) Effective IS Security: An Empirical Study. Information Systems Research 1(3): 255-276.

Straub DW, Carlson PJ & Jones EH (1993) Deterring cheating by student programmers: a field experiment in computer security. Journal of management systems 5(1): 33-48.

Straub DW & Welke RJ (1998) Coping with systems risk: security planning models for management decision making. MIS Quarterly 22(4): 441-469.

Stuart P (1992) Fresh Ideas Energize Reward Programs. Personnel Journal 1992 (January): 111-117.

Systems Security Engineering - Capability Maturity Model (SSE-CMM) (1999) Model Description Document V. 2.0, April 1, 1999. Cited February 9th 2003 from http://www.sse-cmm.org/model/images/ssecmmv2final.pdf.

Telders E (1991) Security awareness programs: a proactive approach. Computer Security Journal 7(2): 57-64.

The International IS Security Foundation (I^2SF) (1999) Generally Accepted System Security Principles, (GASSP) Version 2.0. Cited February 9th 2006 from http://web.mit.edu/security/www/gassp1.html.

Thomson ME & von Solms R (1997) An effective IS security awareness program for industry. Proceedings of the WG 11.2 and WG 11.1 of the TC-11 IFIP.

Thomson ME & von Solms R (1998) IS security Awareness: educating your users effectively. Information Management & Computer Security 6(4): 167-173.

Troy K (1993) Recognize Quality Achievement With Noncash Awards. Personnel Journal (October): 111-117.

Tudor JK (2001) IS security Architecture, An Integrated Approach to Security in the Organization. Auerbach Publications, USA.

Varey RJ (2002) Marketing Communication, Principles and Practice. Routledge, London.

Vroom C & von Solms R (2002) A Practical Approach to IS security Awareness in the Organization. Proceedings of IFIP TC-11 17th International Conference on IS security (SEC2002).

Vyskoc J & Fibikova L (2001) IT users' perception of IS security. Proceedings of the IFIP WG 9.6/11.7 Working-Conference.

Wagel WH (1990) Make Their Day – The Noncash Way!. Personnel 1990 (May): 41-44.

Walls JG, Widmeyer GR & El Sawy OA (1992) Building an Information Systems Design Theory for Vigilant EIS. Information Systems Research 3(1): 36-59.

Walters CG & Grusec JE (1977), Punishment. Freeman, San Francisco.

Weber E & Milliman R (1997) Perceived risk attitudes: Relating risk perception to risky choice. Management Science 43(2): 122-143.

Webster J & Watson RT (2002) Analyzing the past to prepare for the future: writing a literature review. MIS Quarterly 26(2): xiii-xxiii.

White House (2003a) The National Strategy to Secure Cyberspace, Priority III: A National Cyberspace Security Awareness and Training Program. Cited May 4th 2006 from http://www.whitehouse.gov/pcipb/priority_3.pdf.

White House (2003b) The National Strategy to Secure Cyberspace, Appendix: Actions and Recommendations (A/R) Summary. Cited May 4th 2006 from http://www.whitehouse.gov/pcipb/appendix.pdf.

Wood CC (1995) IS security awareness raising methods. Computer Fraud & Security Bulletin (June): 13-15.

Wood CC (2002) The Human Firewall Manifesto. Computer Security Journal 18(1): 15-18.

Yeshin T (1998) Integrated Marketing Communications. Butterworth-Heinemann, Oxford.

Zeckhauser RJ & Viscusi WK (1990) Risk Within Reason. Science 248: 559-563.

∅lnes J (1994) Development of Security Polices. Computers & Security 13: 628-636.

Appendix 1 Information security 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 into your work? If yes, give some examples of what instructions and for what purposes.
4. Did you find the instructions useful for your purposes? Where 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 your applied the information classification rules in your work (i.e., in practice)?
7. How much time do you spend processing email (company's email account) on weekly basis? (Your best estimate)
8. For what purposes do you use email in your work?
9. What do you consider as acceptable use of our company's email system?
10. Give examples of what you consider unacceptable use of our company's email system?
11. Have you ever encountered malicious software in email 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 you receive at your company email account (e.g., on weekly basis)? Give also an estimate (e.g., percentage) of spam messages of all received messages. Have you ever tried to answer any of the spam messages?
14. In your opinion, by what means is it possible to distinguish relevant email messages from spam or other possibly dangerous messages?
15. By what means would you ensure that opening an email attachment is safe?
16. In your opinion, for what reasons in general should digital signing be used when sending email messages via the Internet?
17. In your opinion, what kind of information should be digitally signed in your own work-related email messages?
18. In your opinion, what kind of contents should be encrypted in your own work-related email messages?
19. Do you consider using e-mail encryption and digital signatures to be difficult? Why?
20. Have you ever encrypted work-related email messages? For what reasons did you encrypt them?
21. If the receiver (e.g., a customer company) does not have a compatible email encryption / decryption system, are you able to encrypt information in some other way? How would you do this?
22. Are there any other security viewpoints that you consider important for your work?

Appendix 2 Plan for the first IS security awareness training session at SC

Part 1

- A collaborative discussion concerning threats related to the use of email.
- The aim is to activate learners' existing knowledge about the topic.

Part 2

- Collaborative work in groups of three to five learners.
  - Conducted through exploring documents that the learners have sent to partners and customers using email. We will use authentic email messages sent by the learners.
- Learners' first task is to analyze the above documents and find valuable, sensitive information in them.
- The second task is to explore possible consequences to the company, to the team, and to the learners themselves if the information in these documents is revealed e.g., to competitors, or unintentionally changed or deleted.
- The aim is to make the instruction personally relevant to the learners and in this way to motivate their cognitive processing.
- Another goal is to make the subject matter significant to the self and others, which should motivate learners' cognitive processing.
- The third goal is to build a cause-and-effect mental model to enhance long-lasting learning.
- Instructors' feedback needs to be given instantly to support long-lasting learning results.

Part 3

- A group discussion exploring alternative ways to encrypt emails when S/MIME can not be used.
  - The aim is to find alternative encryption methods for S/MIME.

Appendix 3 Plan for the second IS security awareness training session at SC

Part 1

- Demonstrating and practicing the use of 7zip with the help of the instructor.
- Collaborative group work in groups of three to five learners.
- The aim is to make the employees capable of using 7zip for email encryption.
  - =>The learning task for the first part is to achieve the knowledge and skills required to use 7zip to encrypt emails and to share a password through an alternative communication channel.

Part 2

- Collaborative discussion in one group.
- The goal is to agree upon a simple procedure to protect information on portable devices such as DVDs, CD ROMs and USB tokens.
  - =>The learning task for the second part is to achieve the knowledge and skills required for using 7zip to encrypt files in portable devices.

Appendix 4 Information security questionnaire for planning IS security awareness training at ILC

1. In your opinion, what does the term “information security” mean (i.e. how would you define it)?
2. How do you see the role of information security in your work (i.e. how is information security related to your personal work)?
3. What is the role of information security in your business unit?
4. Who has the responsibility over information security in your business unit?

Appendix 5 Plan for the IS security awareness training session at ILC

Part 1

- A group discussion concerning IS security.
- The idea is to activate the learners' prior knowledge regarding the subject matter.
- In addition, the discussion aims to demonstrate that IS security is an issue of confidentiality, integrity, and availability.
- Furthermore, the aim is to demonstrate that IS security is dependent on employees' behavior.

Part 2

- Collaborative work in groups of three to five employees.
- The first task is to analyze authentic customer documents and find valuable sensitive information in them.
- The next task is to analyze the possible consequences to the company, to the business unit, and to the learners themselves if the aforementioned information is destroyed, changed or revealed to unauthorized recipients.
- The goal is to point out that IS security is a matter of confidentiality, integrity and availability.
- Another goal is to make the subject matter significant to the self and others.
    - This is expected to motivate the learners' cognitive processing.
- An additional goal is to build a cause-and-effect mental model to enhance long-lasting learning.
- Instructors' feedback should be given instantly to support long-lasting learning results.

Part 3

- A group discussion.
- The third part covers factors that have an impact on employees' motivation to protect customers' valuable information.
    - The aim is to emphasize that the behavior and communication of influential people (opinion formers) has an impact on employees' subjective norms and consequently, on achieving good IS security.

Appendix 6 Information security questionnaire for evaluating IS security awareness training at ILC

1. How do you see the e-Learning package and its IS security test from the viewpoint of your learning and your own work (i.e., how useful and relevant was the package for your learning and for your work)?
2. Regarding the e-Learning package, what was good and what was bad?
3. How did you find the training session from the viewpoint of your learning and your own work?
4. Regarding the training session, what was good and what needs further improvement?
5. How do you feel about the IS security guidelines presented in the training?
6. Has the training session had any impact on your thoughts about IS security?
7. Has the training session influenced your thoughts about your work?
8. Has the training session had an impact on your ways of working (regarding IS security issues)?
9. Do you have any feedback to give the trainers or your manager regarding the training session or any other IS security issue (e.g., in your business unit)?

448. Ylianttila, Mari (2005) Structure-function studies of the peroxisomal multifunctional enzyme type 2 (MFE-2)

449. Moisio, Kari (2005) Numerical lithospheric modelling: rheology, stress and deformation in the central Fennoscandian Shield

450. Pöykkö, Heikki (2005) Host range of lichenivorous moths with special reference to nutritional quality and chemical defence in lichens

451. Kinnula, Marianne (2006) The formation and management of a software outsourcing partnership. A case study

452. Autio, Jyrki (2006) Environmental factors controlling the position of the actual timberline and treeline on the fells of Finnish Lapland

453. Rautiainen, Pirjo (2006) Population biology of the *Primula sibirica* group species inhabiting frequently disturbed seashore meadows: implications for management

454. Taskinen, Jukka (2006) Protein crystallographic studies of CoA-dependent proteins: new insight into the binding mode and exchange mechanism of acyl-CoA

455. Molin-Juustila, Tonja (2006) Cross-functional interaction during the early phases of user-centered software new product development: reconsidering the common area of interest

456. Thomson, Robert L. (2006) Breeding habitat selection and its consequences in boreal passerines. Using the spatial dispersion of predators and heterospecifics as a source of information

457. Iivari, Netta (2006) Discourses on 'culture' and 'usability work' in software product development

458. Vähäoja, Pekka (2006) Oil analysis in machine diagnostics

459. Mutanen, Marko (2006) Genital variation in moths—evolutionary and systematic perspectives

460. Bhaumik, Prasenjit (2006) Protein crystallographic studies to understand the reaction mechanism of enzymes: α-methylacyl-CoA racemase and argininosuccinate lyase

461. Korkalo, Tuomo (2006) Gold and copper deposits in Central Lapland, Northern Finland, with special reference to their exploration and exploitation

462. Pahnila, Seppo (2006) Assessing the usage of personalized web information systems

Book orders:
OULU UNIVERSITY PRESS
P.O. Box 8200, FI-90014
University of Oulu, Finland

Distributed by
OULU UNIVERSITY LIBRARY
P.O. Box 7500, FI-90014
University of Oulu, Finland

UNIVERSITY OF OULU P.O. Box 7500 FI-90014 UNIVERSITY OF OULU FINLAND

ACTA UNIVERSITATIS OULUENSIS

ISBN 951-42-8113-6 (Paperback)
ISBN 951-42-8114-4 (PDF)
ISSN 0355-3191 (Print)
ISSN 1796-220X (Online)