MIS Quarterly

RESEARCH ARTICLE

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

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

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

# Appendix A

## A Questionnaire for Planning IS Security Awareness Training at SC

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

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

# Appendix B

## Methodological Details

### *Principles for Conducting the Research Interviews*

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

### *Principles for Evaluating the Validity of the Action Research Intervention*

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

# Appendix C

## Evaluating the Interventions from the Viewpoint of Action Research Validity Criteria

**Table C1. Action Research Validity Criteria**

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

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

## *References*

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

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

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

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

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