A case study in information security awareness improvement: a short description

Isabella CORRADINI
Themis Research Centre
Roma, Italy

and

Enrico NARDELLI
Univ. Roma "Tor Vergata"
Roma, Italy

ABSTRACT

In this paper we provide a short description of a training experience aiming at improving information security awareness. It has been conducted in a multinational company operating in the electronic payments sector. The overall training effort has been based on an organizational analysis and a survey on cyber risk perception involving 1164 employees. The survey pointed out the needs of strengthening education and training in internal cooperation, socio-technical awareness of cyber risks, risk profiling and management.

Keywords: Security Awareness, Risk Perception, Organizational Culture, Integrated Methods.

1. INTRODUCTION

An effective application of the concept of awareness to information security issues requires to adopt an interdisciplinary approach integrating technical and human aspects. To obtain awareness, one has to use technologies in an informed way; it is therefore necessary to work on the attitude and motivation of the people so as to induce them to engage attentive behaviors on information security [1, 2, 6].

Our baseline is the importance of analyzing the perception of risk [9, 10] within companies as a foundation for developing their awareness on security issues. In this paper we discuss a survey on the cyber risk perception in employees of a multinational company operating in the area of design, building and management of technology services and infrastructures in the sector of electronic payments and briefly examine its results. This survey is part of the "Risk Culture" educational path that we designed jointly with the company for the training of their entire workforce. By risk culture we mean "the values, beliefs, knowledge and understanding about risk, shared by a group of people with a common intended purpose, in particular the leadership and employees of an organization" [8]. Our point of view is that to develop long-term awareness it is necessary to integrate awareness into the organizational culture [7].

2. METHODOLOGY

The execution of the "Risk Culture" educational path has seen the development of an organizational analysis, a survey on cyber risk perception, training seminars on security and awareness, and other information dissemination actions as posters, publications on the intranet, security tips, videos with testimonials, security days. Literature suggests integrated methods to develop and awareness on information security [3, 4, 5, 11].

The cyber risk perception survey investigated the organizational structure in its various aspects, its

strengths and weaknesses, so as to build a risk culture education path tailored to the specific company.

The tools used for the analysis of cyber risk perception consisted of an analytical questionnaire (designed specifically for this project) with 14 questions of different typology (single choice, multiple choice, and Likert scale answers) and an open ended investigation based on free associations of words. These were 4 open questions asking to freely associate one term to each of the proposed keywords, referring to human aspects central for our psycho-social goals.

The perception of the staff has been investigated in these three areas:

1. Risks in the organization and in the private life
2. Factors affecting the perception of risk;
3. Actions and behaviors for prevention.

3. MAIN RESULTS

Participation in the survey was very high (62,7%) corresponding to 730 completed and analyzed questionnaires out of a total of 1164 administered ones. The majority of the sample is composed by male (more than 65%) and the most represented age group is between 41 and 50 years.

The strongest element emerged from data analysis has been that the company already has a solid awareness with respect to three issues:

- the importance of the role played by people in all stages of risk management,
- the key role of communication,
- the need of organizational preparedness.

We now describe, just as an example, one survey question in each of the three investigated areas.

In area 1, a multi-question asked to employees to evaluate on a 1 ("*negligible*") to 5 ("*very high*") scale the expected impact on their company of a number of factors. The three of them which resulted, in the average, to have the highest value have been:

- Data breaches (4.3)
- Frauds (4.06)
- Attacks against IT Infrastructures (4.03)

where 4 corresponds to a value of "*high*".

With respect to area 2, a question asked to pick the single most important factor affecting people's perception of risky situation. The three most selected ones among the four proposed factors have been:

- Personal ability to manage the situation (37,7%)
- Personal interest with respect to the situation (28,4%)
- Emotions emerging in the situation (24,7%)

In area 3, a question asked to select the three most important actions to implement in an organization for an effective prevention of cyber risks. Those selected as the most important ones in a pool of nine possible choices have been:

- Risk analysis (selected by the 64% of the sample)
- Continuous education and training (59%)
- State of the art technologies (43%)
- Clear and timely internal communications (41%)

For what regards the qualitative part of the survey we briefly examine the outcomes of just one of the investigated keywords: *trust*.

We standardized the terms associated in the answers to the keyword by first "stemming" them (that it, by bringing each term back to its root) and then coalescing synonyms and semantically close terms.

The keyword "*trust*" is mainly associated with security (10% of respondents have chosen this term) followed by reciprocity (6%) and reliability (4%), which were the three terms with higher frequency. Note that since terms for answers could be freely chosen, there was a very large number of them: about a hundred.

4. DISCUSSION AND FUTURE WORK

Summarizing the overall results, the survey pointed out the need of strengthening employees education and training in the following areas:

- Cooperation and information sharing
- Knowledge of integrated socio-technical methods to deal with cyber risks
- Deeper understanding of risks induced by information processing technologies
- Deeper understanding of risk profiling and management methods

Given the periodical enter of new staff and the evolution of technology the "Risk Culture" educational path will become a semi-permanent activity. We are now designing and implementing a monitoring process to measure the actual effects of the educational path on the employees.

9. REFERENCES

[1] Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", **MIS Quarterly**, Vol.34, N.3, pp. 523-548, September.

[2] D'Arcy, J., Hovav, A., and Galletta, D. (2008). "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach", **Information Systems Research**, 20:1, pp.79-98.

[3] Herold, R. (2010). "**Managing an Information Security and Privacy Awareness and Training Program**", CRC Press, Taylor&Francis. Second edition.

[4] Kruger H. A., Kearney W. D., "A prototype for assessing information security awareness", **Computers & Security** 25, 289-296, 2006.

[5] Maqousi, A., Balikhina, T., Mackay, M. (2013). "An Effective Method for Information Security Awareness Raising Initiatives", **International Journal of Computer Science & Information Technology** (IJCSIT), Vol.5, No.2, April.

[6] Siponen, M. T. (2000). "A Conceptual Foundation for Organizational Information Security Awareness", **Information Management & Computer Security**. Vol.8, Issue 1.

[7] Spurling, P. (1995). "Promoting Security awareness and commitment", **Information Management & Computer Security**, Vol. 3, No.2, pp. 20-26.

[8] The Institute of Risk Management: Under the Microscope. Guidance for Boards, https://www.theirm.org/media/ 885907/ Risk_Culture_A5_ WEB15_Oct_ 2012.pdf

[9] Slovic, P. (1987), "**Perception of Risk**", Science, Vol.236, Issue 4799, pp.280-285.

[10] Slovic, P. (2000). "**The perception of risk**", Earthscan Publications.

[11] Wilson, M. and Hash, J. (2003). "**Building an Information Technology Security Awareness and Training Program**", Computer Security, NIST, Special Publication 800-50.