INFORMATION SECURITY CULTURE
–
FROM ANALYSIS TO CHANGE

Thomas Schlienger, Stephanie Teufel

iimt (international institute of management in telecommunications)
University of Fribourg

thomas.schlienger@unifr.ch
+41 26 300 84 28
stephanie.teufel@unifr.ch
+41 26 300 84 35

iimt
Université de Fribourg
Av. de Tivoli 3
CH-1700 Fribourg

ABSTRACT

Information Security Culture includes all socio-cultural measures that support technical security methods, so that information security becomes a natural aspect in the daily activity of every employee. To apply these socio-cultural measures in an effective and efficient way, certain management models and tools are needed. In our research we developed a framework analyzing the security culture of an organization which we then applied in a pre-evaluation survey. This paper is based on the results of this survey. We will develop a management model for creating, changing and maintaining Information Security Culture. This model will then be used to define explicit socio-cultural measures, based on the concept of internal marketing.

KEY WORDS

information security culture, information security awareness, information security marketing, evaluation of information security culture, change and maintenance of information security culture

INFORMATION SECURITY CULTURE
–
FROM ANALYSIS TO CHANGE

1. INTRODUCTION

In our research on Information Security Culture, we developed a method-mix framework that we applied in our survey at the telecommunications company Orange Switzerland (Schlienger and Teufel 2003). This framework will be discussed briefly and the main results of the survey will be presented. We asked all employees how they understand the security policy of Orange Switzerland. The results impressively show, that the security policy is known in general, but not supported in all points, neither by the employees nor by the management. It also shows, that the employees need extra security training and education. Security at Orange Switzerland is managed only on a technical and an organizational level. Socio-cultural aspects are missing. Methods to create, maintain and to change the security culture are therefore needed.

Based on this insight, we will develop an Information Security Culture management model in this paper. Also, the life cycle of the security culture has to be considered, since its different stages need different management methods. Radical management methods should be used to create or change culture, whereas more subtle methods are needed to maintain an appropriate culture. With the cultural management model and the results of the culture survey, we will define an action plan to change and maintain security culture.

Information Security Culture is a part of the organizational culture. Before going on in the discussion of how to manage security culture, we give a short definition of organizational culture. From it, we deduce the concept of Information Security Culture. For a more detailed discussion of our Information Security Culture concept see (Schlienger and Teufel 2002).

1.1. Definition of Information Security Culture

Organizational culture defines how an employee sees the organization (Ulich 2001). It is a collective phenomenon that is growing and changing over time and, to some extent, it can be influenced or even designed by the management.

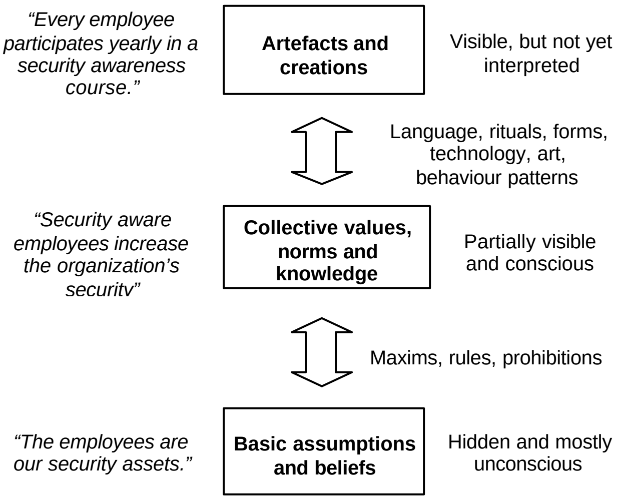
"Every employee participates yearly in a security awareness course."
Artefacts and creations
Visible, but not yet interpreted
Language, rituals, forms, technology, art, behaviour patterns
"Security aware employees increase the organization's securitv"
Collective values, norms and knowledge
Partially visible and conscious
Maxims, rules, prohibitions
"The employees are our security assets."
Basic assumptions and beliefs
Hidden and mostly unconscious

***Figure 1.* The three Layers of Information Security Culture, see (Schein 1985)**

The two core substances of the organizational culture are basic assumptions and beliefs. The organizational culture is consequently expressed in the collective values, norms and knowledge of organizations. In turn, those collective norms and values affect the behaviour of the employees. Artefacts and creations such as handbooks, rituals and anecdotes are the expression of such norms and values. Ultimately, the organizational culture has a crucial impact on the corporate success (Rühli 1991). Organizational culture emerges and grows with time. It is formed by the behaviour of dominant organization members like founders and top managers.

An organizational culture can have different subcultures based on suborganizations or functions. Information Security Culture is a subculture in regard to general corporate functions. It should support all activities in a way, that information security becomes a natural aspect in the daily activities of every employee. The three layers of Information Security Culture and their interactions are illustrated in Figure 1.

2. MANAGING INFORMATION SECURITY CULTURE

Information Security Culture, like organizational culture, can't be created once and then be used all life time. To ensure that it corresponds with the targets of the organization and that the organizational members don't forget it, culture must be created, maintained or changed continuously. It's a never ending process, a cycle of evaluation and change or maintenance. The first step is to analyze the actual Information Security Culture (pre-evaluation). If the culture doesn't fit with the organization's targets the culture must be changed. If it fits, it should be reinforced. The success of the actions taken must then be controlled (post-evaluation). This cycle is illustrated in Figure 2.

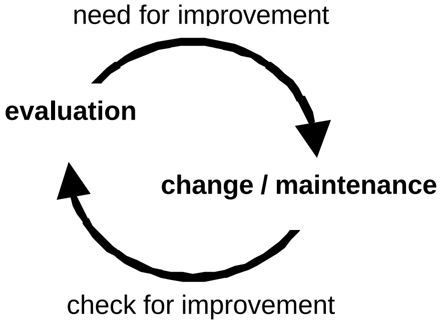

Figure 2. **The Information Security Culture Management Cycle**

Having a closer look to this cycle of Information Security Culture management, we can identify the following five phases, see also (Bruhn 1999):

1. Pre-Evaluation
2. Strategic Planning
    a. Definition of targets
    b. Segmentation of organizational members
3. Operative Planning
    a. Instruments of internal marketing
    b. Instruments of human resources management
    c. Instruments of organizational development
4. Implementation
5. Post-Evaluation

This proposed process is very similar to the internal marketing concept. Like in internal marketing, security culture management wants to promote certain values, corporate goals and philosophies within an organization. We want to "sell" information security aware behaviour to our employees. The methods of internal marketing creates advantages in competition by promoting and creating the understanding and engagement of the corporate goals all over the organization (Bruhn 1999; Purtschert 2001).

3. EVALUATION

In order for security culture to make a substantial contribution to the field of information security, it is necessary to have a set of methods for studying security culture. Unfortunately, no unique toolset and method for the study of organizational and therefore security culture exists. Research is therefore still needed in this field. The researcher must solve two main questions:

1. **What to analyze**: according to the used cultural model, one could measure the collective values, norms and knowledge, or, one could measure the cultural indicators, the artefacts. Basics assumptions are a priori not feasible.

2. **How to analyze**: for the measurement of observable indicators, social sciences often propose to analyze documents, to observe of physical indicators and to interview organization's members. For the measurement of norms, values and beliefs, it is proposed to use narrative interviews, participative observations and group sessions.

A more detailed discussion of the evaluation items (what) and methods (how) can be found in (Schlienger and Teufel 2003). Bearing in mind the difficulties to comprehend culture at all, it seems evident to use a combination of measuring items and methods as proposed among others by (Rühli 1991; Schreyögg 1999; Vecchio 2000). This allows to verify the results with other methods and to use different viewpoints in interpreting them. The researcher is now able to pick the appropriate methods, which help him assess the security culture in his/her organization. In our research we use the following method-mix illustrated in Table 1.

Table 1. **Items and Methods for evaluating Information Security Culture**

Method **Item**	Analysis of documents	Questionnaire	Group session	Interview	Observation
Artefacts	Analysis of the security policy			Interview with the Chief Security Officer (CSO)	Audit
Official values		Questioning all level of employees			
True values					

The concrete approach we use in our research project at Orange Switzerland (see also (Schlienger and Teufel 2003)) is named in the grey-shaded box. In our project we focus on the security attitude and perception of the employees, without specific analysis of information security management and concepts. Therefore, the main target of the questionnaire with its ten questions is to find out the following: Do the employees know, what the security policy states and do they support it? We strictly followed the main points of the policy in our analysis. Each question has three sub-questions (see example question in Table 2): a) individual attitude (true values), b) perception of company's attitude (official values: security policy) and c) best solution. This trichotomy will give interesting insights and reveal gaps between the individual's and the company's perception. It also has a didactic impact, since the user has to reflect upon the best solution.

Table 2. **Example question**

2	The computer and electronic communications systems should be used for Orange's business activities only.			
	a) Personally I think, this is	True	False	I don't know
	b) Orange regards this as	True	False	I don't know
	c) If I were responsible, I would regard this as	True	False	I don't know

The whole process has been supported by several unstructured interviews with the Chief Security Officer of Orange Switzerland, which whom we discussed the security policy and the findings of the survey. Audits to verify the given answers and the real behaviour are in the planning stage.

3.1. Need for Improvement

To identify the main gaps between the policy and the perception of the employees, we used the statistical factor analysis interpreting the answers of the questionnaire. Factor analysis is used to reduce a given set of variables (in our case the 30 answers of the questionnaire) to a smaller independent set of factors. Our analysis identified 11 factors. 10 factors are identical to the 10 questions. One factor is new and includes 4 sub-questions concerning the official policy (sub-question b) in the fields of: encryption of confidential emails (question 6), security training (question 7), management buy-in (question 8) and role of security policy (question 9). In the descriptive analysis of the answers (see Figure 3), these four sub-questions were also identified as main problems.

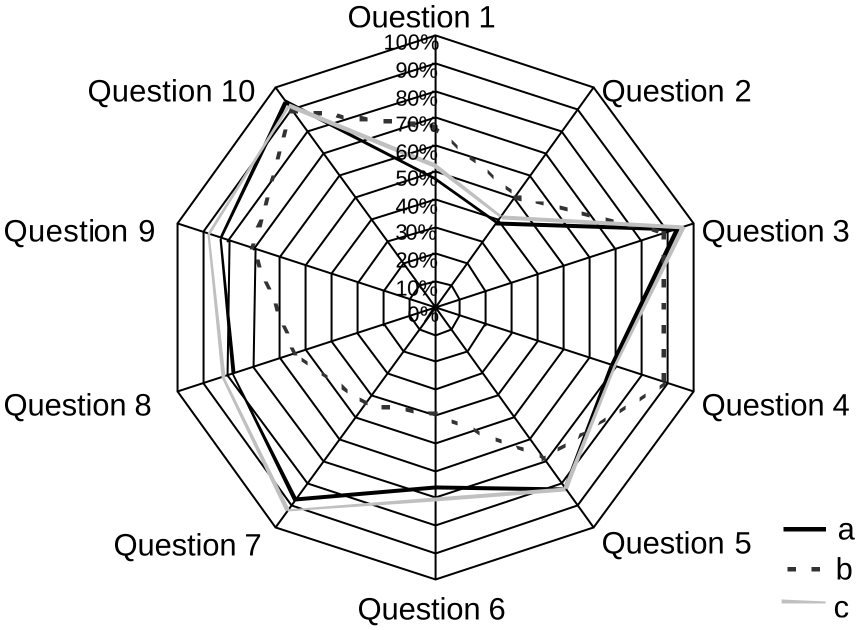

Figure 3. **Information Security Culture Radar**

The results of the evaluation show, that the security policy is known in general, but not supported in all points, neither by the employees nor by the management. It also shows, that the employees need extra security training and education. Security at Orange Switzerland is managed only on a technical and on an organizational level. Socio-cultural aspects are missing. Methods to create, maintain and to change the security culture are therefore needed.

4. STRATEGIC PLANNING

The evaluation stage revealed the actual culture and its problems. Depending on the target culture, specific actions must be taken to maintain or even change the culture. It must be considered, that changing an existing culture needs more radical measures than maintaining an appropriate culture. Whereas an appropriate security culture can be maintained by a good awareness-program, possibly in combination with the existing course-program, in order to change a culture, all existing cultural measures must be reengineered.

4.1. Targets

Clear objectives for the development of an appropriate security culture must be set. In our project the target security culture is defined by the security policy. It is a superior document for all measures concerning information security and defines the basics for the security behaviour. Defining a target culture isn't based on a clear top-down approach. A security policy shouldn't be developed independently from real life. It depends on the actual corporate culture and the manifested work processes. A pre-evaluation may request to redo the security policy first. In our esearch we found some weak points in the security policy that should be eliminated above all else. Only afterwards can the security policy be used as the superior security culture document.

4.2. Segmentation of Organizational Members

To be able to define the right cultural measures, you must know the people you want to influence. A widely used approach is to define the three groups IT-staff, managers and employees and to implement special measures for each one. In our research, the segmentation by function (IT vs. business) or position (employee vs. manager) revealed statistical significant differences that ask for defining special cultural measures for specific departments or management levels.

Another method to segment the organization members is applying statistical cluster analysis. Cluster analysis composes different groups the way, that the group members have as similar attributes as possible. In our case the cluster analysis defined four different groups. According to their answer patterns we named them:

- **"I'm happy"-Cluster:** These people are happy with the security policy and seem to follow the defined rules (44% of answers).

- **“Danger comes from outside”-Cluster:** These people see all the dangers outside the company and don’t care what is going on within the company. Information security lies in the responsibility of the security staff who has to protect the company from outside dangers (19% of answers).

- **“Careless people”-Cluster:** These people don’t see any problem and consider security policies and rules as needless (4% of answers).

- **“I’m unhappy”-Cluster:** These people are unhappy with the actual policy and would like to have more security (32% of answers).

Clustering the people will help the security personnel a lot when choosing the appropriate instruments and defining the appropriate measures for the right target group.

5. OPERATIVE PLANNING

Comparing the actual with the target security culture, one can choose the right instruments to implement the target culture. Culture cannot be decreed by regulations, more subtle actions are possible and necessary. We want to discuss three exemplary main instruments. On the basis of internal communication, training, education and exemplary acting of managers, a culture can be developed step by step. The aim of the cultural measures is to encourage the security awareness of the management and employees. Increased awareness creates and supports a good security culture.

5.1. Internal Communication

Every cultural measure is based on the theory of internal communication, an instrument of the corporate communication. Internal communication enables the company to share information, knowledge and motivation, to take the dialog between top management and employees and to get feedback. It creates acceptance and gets commitment for the corporate targets and strategies (Bruhn 1999; Meier 2000). Internal communication has the following functions:

- **Informational functions:** to rule, coordinate and orientate

- **Dialog functions:** to orientate and contact

Also two main forms of internal communication can be identified; we added the most common instruments of each:

- **Interpersonal communication:** discussion between employee and employer, seminars, training and workshops

- **Communication via medias:** corporate newspaper, intranet, guidelines and black board

A good cultural program needs the right mixture of communication instruments. We will now discuss three important instruments in more detail.

5.2. Management-Buy-In

Before implementing a security training and awareness program, you must convince the management of the importance of information security. The inherent problem of information security is that one cannot calculate the revenue of security investments. To be able to convince management anyway, (Haller 1990) proposes the risk dialog. Objective arguments, like statistics or references, can help to convince management. Emotional argumentation like examples, comparisons or suggestions can also motivate management to support information security. Our "rational" decisions are often based on our feelings, even if we argument objectively (Braun 2001).

5.3. Security Awareness and Training Program

Schooling is one of the core elements to create security awareness. It is vital to implement the security policy. The Chief Security Officer is responsible to develop the appropriate schooling program and/or to implement security elements in the existing IT schooling program. A security training and awareness program can be divided in three different parts, see e.g. (Tudor 2000; Horrocks 2001):

- **Education:** The employee must understand, why information security is important for the organization. He/she must understand, that everybody is responsible for security in his/her own sphere of influence. Education can be implemented e.g. with a special information security course. It can also be basic information security education in schools and universities, as proposed by (Horrocks 2001).

- **Training:** The employee has to know, how he/she can behave secure. He/she must know, how to use the security functions within the applications and in the own work process. Training of special security tools or features within applications must be offered.

- **Awareness:** Education and training are the basis for the security program. However, they don't guarantee security conform behaviour in daily work life. Awareness measures outside of the class room remember the employees on the lessons learnt. Gadgets like posters, mouse-pads and pens with security slogans help to make the security topic omnipresent. Incentive and suggestion systems encourage the employees to participate. Controls, obligations and penalties show the importance of information security.

The security awareness and training program leads from “become aware” to “stay aware” and ends up in “be aware”, which changes a security culture definitively.

6. IMPLEMENTATION

The implementation of information security can be divided in the following four stages, illustrated in Figure 4.

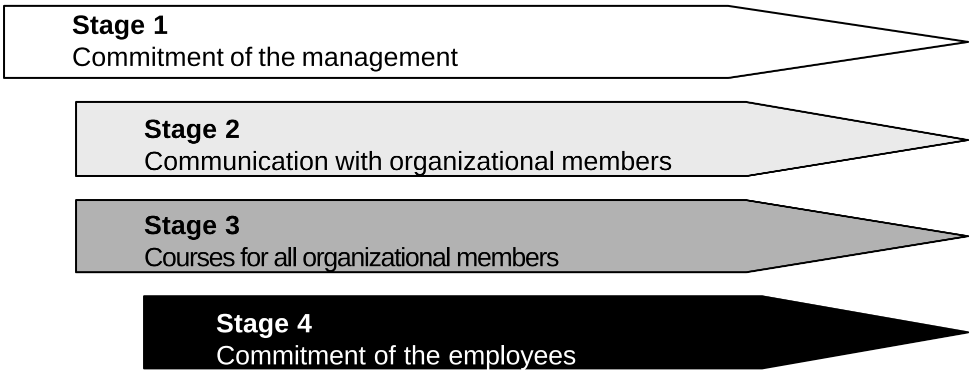
Stage 1
Commitment of the management
Stage 2
Communication with organizational members
Stage 3
Courses for all organizational members
Stage 4
Commitment of the employees

***Figure 4.* The four Stages of Information Security Culture Implementation**

Stage one prepares the management to the topic of information security and gets their commitment. Next, the understanding and acceptance for the topic must be get from all employees. Open dialog and discussion between management and employees are important in this stage. Also, in stage three the organizational members are trained and educated. The last stage guides to a lasting change of security culture, it includes omnipresent awareness campaigns and specific security rules. These four processes run parallelly with slightly different starting times.

For implementing Information Security Culture, we can use the well known four P’s of the marketing-mix, see e.g. (Purtschert 2001; Kotler 2003). These P’s define four instruments which help to design the relationship between the different players and in the same time change the behaviour of the target group. We shortly discuss the four P’s and give some examples, how they could be used for Information Security Culture management.

6.1. Product

The “product” we want to sell is information security. This product must have a specific quality and packaging to get the attraction of the employees. Security tools must have a high usability, and policies, manuals and courses must be attractive and motivating.

6.2. Price

We don't understand price as real costs, but the psychological expenditure to learn new tools and processes. This expenditure can be very high, because organizational members have to learn new conduct without receiving a direct return. The organization has to install appropriate incentive systems to lower the "price" of security.

6.3. Place

Place defines the distribution channels and the distribution organization. The organization defines, who implements the security culture measures: internal or external specialists? This question depends on the internal know-how and resources. The organization defines also the cooperation of departments, like IT, marketing and human resources. The distribution channel defines weather the organization uses direct or indirect channels. In direct channel, e.g. the chief security officer trains and educates himself, whereas the individual department managers get more involved in the indirect channel.

6.4. Promotion

Promotion defines the different ways that could be used to communicate information security, as we have discussed already in chapter 5. Which media do we use to communicate the message of information security? It is also indispensable to create a specific security logo and slogan, that will be used in every security context.

7. SUMMARY

The research work presented in this paper defines a model for managing Information Security Culture and an action plan that helps to change and maintain Information Security Culture in an organization. The model is based on the results of a pre-evaluation Information Security Culture survey at the telecommunications company Orange Switzerland and on the theory of internal marketing. We discussed the five main phases: pre-evaluation, strategic planning, operative planning, implementation and post-evaluation. The implementation phase can be separated in the four different stages management commitment, internal communication, know-how transfer and employee commitment. The four marketing P's product, price, place and promotion help to design these stages operatively.

Whereas the evaluation phase has already been conducted successfully, implementation of security culture measures isn't done yet. Practical experience has to show, if the proposed method can change or maintain an appropriate Information Security Culture.

8. ACKNOWLEDGEMENT

We thank Mr. Daniel Hallen from Orange Switzerland for his ongoing cooperation in our Information Security Culture project. We also thank the students of the course “management in telecommunications 2003” for their valuable contribution: Arnold Natalie, Borter Patrick, Corabianu Dinu, Fraser André, Giger Dominic, Krieger Manuel, Künzli Josef, Sieber Karin, Unterberger Claudius.

9. BIBLIOGRAPHY

Braun, R. (2001). Die Macht der Rhetorik: besser reden - mehr erreichen. Frankfurt, C. Ueberreuter.

Bruhn, M. (1999). Internes Marketing als Forschungsgebiet der Marketingwissenschaft. Eine Einführung in die theoretischen und praktischen Probleme. In: M. Bruhn, Ed. Internes Marketing: Integration der Kunden- und Mitarbeiterorientierung. Grundlagen - Implementierung - Praxisbeispiele. Wiesbaden, Gabler. **2. Auflage:** 15-44.

Haller, M. (1990). Risikodialog. In: R. Königswieser and C. Lutz, Eds. Das systemisch-evolutionäre Management. Wien, Orac-Verlag.

Horrocks, I. (2001). "Security Training: Education For an Emerging Profession?" Computers & Security **20**(3): 219-226.

Kotler, P. (2003). Marketing management. Upper Saddle River, N.J, Prentice Hall.

Meier, P. (2000). Interne Kommunikation von Unternehmen: theoretische und empirische Aspekte zur Organisation und Sprache der Internen Kommunikation grosser Unternehmen in der Schweiz. Zürich.

Purtschert, R. (2001). Marketing für Verbände und weitere Nonprofit-Organisationen. Bern, Haupt.

Rühli, E. (1991). Unternehmungskultur - Konzepte und Methoden. In: E. Rühli and A. Keller, Eds. Kulturmanagement in schweizerischen Industrieunternehmungen. Bern und Stuttgart, Paul Haupt Verlag**:** 11-49.

Schein, E. H. (1985). Organizational Culture and Leadership: A Dynamic View. San Francisco, Jossey-Bass.

Schlienger, T. and S. Teufel (2002). Information Security Culture - The Socio-Cultural Dimension in Information Security Management. In: M. A. Ghonaimy, M. T. El-Hadidi and H. K. Aslan, Eds. Security in the information society: visions and perspectives. IFIP TC11 International Conference on Information Security (Sec2002), Cairo, Egypt, Kluwer Academic Publishers.

Schlienger, T. and S. Teufel (2003). Analyzing Information Security Culture: Increasing Trust by an Appropriate Information Security Culture. unpublished, accepted on the TrustBus'03 workshop in conjunction with the 14th International Conference on Database and Expert Systems Applications (DEXA 2003).

Schreyögg, G. (1999). Organisation: Grundlagen moderner Organisationsgestaltung. Wiesbaden, Gabler Verlag.

Tudor, J. K. (2000). Information security architecture. Boca Raton, FL, Auerbach.

Ulich, E. (2001). Arbeitspsychologie. Zürich, vdf, Hochschulverlag an der ETH Zürich.

Vecchio, R. P. (2000). Organizational behavior : core concepts. Fort Worth, Dryden Press.