15

INFORMATION SECURITY CULTURE
The Socio-Cultural Dimension in Information Security Management

Thomas Schlienger, Stephanie Teufel
iimt - international institute of management in telecommunications
University of Fribourg (CH)

Abstract: The information security management mostly disregards the human dimension. The main focus is on technical and procedural measures. The user is seen as a security enemy, not as a security asset. In our paper we identify some problems, that emerge from this sight and we propose a paradigm shift from a technical approach to a socio-cultural one, from "the user is my enemy" to "the user is my security asset" approach. We explain the concept of corporate culture and show exemplary on the example of the security culture, how the cultural theory can help to increase the overall security of an organization.

Key words: Security Culture, Awareness, Human Dimension, Information Security Management

1. MOTIVATION

In the information security discussion the human dimension is mostly disregarded. The main focus is on technical security measures where users are seen as a threat for information security. As of this technical focus, the possibilities of information security measures are mostly used in an unsatisfactory way. In our paper we propose a paradigm shift from a technical to a human centric focus, from "the user is my enemy" to the "my user is my security asset". We are not yet in a position to give final answers and guidelines to this new approach in information security management, but in this paper we will discuss some aspects, that can help to build a security management, which also takes the human dimension in account.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35586-3_46

M. A. Ghonaimy et al. (eds.), *Security in the Information Society*

Worldwide, the ARIS Attack Registry and Intelligence Service [Attack Registry & Intelligence Service (ARIS) 2001] registered over 90 Mio incidents in the time from 1.1.01 to 23.10.01. In those incidents, over 9'000 different attack types from over 1.5 Mio different IP addresses were launched. Another example is the 23.10.2001. On that day alone, over 200'000 attacks were registered worldwide.

The 2001 Computer Crime and Security Survey from the Computer Security Institute & the FBI [Computer Security Institute 2001, 14], is trying to quantify the loss resulting from the different attacks. In the study 35% of the surveyed organizations were able to give exact numbers of their loss, which amounted to an overall loss of 378 Mio USD. This averages on 2 Mio USD per organization. The most expensive attacks or frauds were:

1. Theft of proprietary information
2. Financial fraud
3. Virus attacks
4. Insider net abuse

Asking about the perpetrators, the study reports that 49% of the incidents were done by insiders. Another study, conducted by the magazine InformationWeek and PricewaterhouseCoopers [Gerbich 2001], lists a detailed analysis of the perpetrators. In 54% of the threads worldwide, insiders were involved. Of those, 23% were authorized users, 16% were unauthorized users and 15% were former employees.

The organizations are able to directly influence these people. Security actions aiming at this group should therefore help to decrease the internal amount of perpetrators. In the first place potential employees should be screened thoroughly, with simultaneous consideration of individual privacy and the data protection law. This proper selection of future employees can improve the security of the organization greatly. It should be avoided to hire unmotivated or malicious staff. Secondly, the hired people must be educated and encouraged to behave in correct manners and thus support the organizational information security. *Figure 1* illustrates this idealized approach. In addition, highly motivated and qualified people also help to decrease external threads such as email viruses and worms.

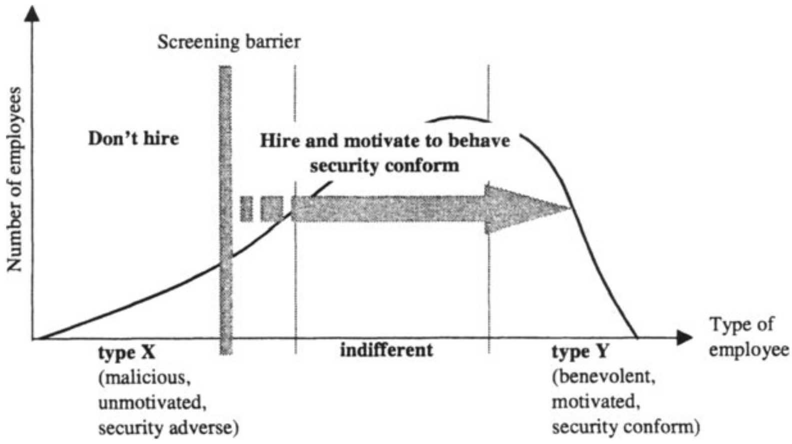

Figure 1. Screening and motivating employees with regards to information security

In General, the number of security incidents increased highly during the last years and organizations increasingly risk to loose money and reputation. Therefore information security has become a critical success factor for organizations. In this approach, the employees play a primary role. In the following chapters we show a possibility for an organization, to turn its employees into valuable security assets. First, we briefly show the development of information security management over the last decades with its rather technical approach. We will then present a method to increase the overall information security of an organization based on organizational and industrial psychology.

2. THE STATE OF THE ART IN INFORMATION SECURITY MANAGEMENT

Today's information security management is based on mistrust and has a highly technological focus. Technical measures are set up to intercept intruders at the gate, to protect the user from making mistakes and to prevent misuse. During the last years security specialists agreed upon the fact, that security management can only be successful if it is embedded in an organizational and managerial structure within the organization. [von Solms 2000, 615] has identified three waves in the developments of information security management.

The first wave was completely based on technical measures and lasted until the beginning of the eighties. Employees were declared to be security risks. The organization had to decrease this risk using technical measures.

Security was primarily seen as a technical problem that had to be solved by technicians using technology. The main development was the implementation of access controls lists, user-ids and passwords.

The start of the second wave can be identified in the early eighties and had its focus on managerial and organizational aspects. Managers got involved in the security process, security responsibles were declared and incorporated into the organizational chart (e.g. chief security officer, CSO). Security policies and concepts were developed in parallel.

Nevertheless as the examples in the introduction show, these technical and procedural measures are not sufficient; socio-cultural measures are also needed. The last link in the security chain is the user who works with the information technology. To him security is laborious and unnecessary [Adams and Sasse 1999, 43]. Today the main problems are, among others, the missing usability of security products and procedures and the organization's mistrust against it's own employees.

For the last years of the nineties, [von Solms 2000, 615] identified a third wave, building up a technical, procedural and socio-cultural security infrastructure: the wave of institutionalisation. It consists of several parts: standardization, certification, metrics and security culture. The latter concentrates on the human dimension in information security, which we want to discuss in depths.

3. THE HUMAN DIMENSION IN INFORMATION SECURITY

Let's give a short example, why users play an important role in information security:

A traditional way to protect information systems is the use of passwords. According to the study of [Furnell, et al. 2000, 533-535] 91% of all systems use passwords, despite the existence of alternative techniques, which are more secure and also more usable. Around 38% of the users have to memorize four or more passwords for their daily work. Some 46% of the users have to change their passwords at least once every six month. Although passwords are unpractical (especially if you have to memorize several of them) and tend to be insecure (especially if you write all your passwords on a note and hide it under the keyboard or if you use very simple passwords), users like them. The study compared the acceptance of passwords with biometric authentication. Authentication using physical attributes doesn't require anymore to remember passwords, thus reducing the mental overhead of the users and thus tending to be more secure, because users don't choose simple passwords or write them down. While 95.7% of the users still preferred passwords, only 53.4% preferred voice recognition, 49.1% face recognition and 48.8% fingerprint recognition. Why don't accept users more comfortable and secure authentication technologies? One clue might come from the fact, that criminal records normally include fingerprints. The scanning of fingerprints can have therefore a negative touch in European countries. An organization simply cannot implement a biometric authentication mechanism if the users do not support them. The rollout of new security products and procedures can only be successful, if firstly the users understand the why's and the how's, and secondly if the users can be motivated to support such a change.

In another study about user's security behaviour, [Adams and Sasse 1999, 42] identified the user's perceptions of organizational security and information sensitivity as one of the four major factors influencing effective password usage. In their study they showed clearly, that users are not sufficiently informed about security issues and that the security departments lacks the knowledge about users.

The following *Table 1* shows a summary of today's information security management problems. It also includes some ideas for future improvements.

Table 1. Problems of information security management and ideas for improvements

Problems	Ideas for improvements
Security products and procedures tend to be unusable	Security engineers should start their design from the users perspective and not from a technological perspective
The user doesn't know the risks of information technology	The user should be informed about the risk of information technology
The user doesn't understand the security measures / techniques	The user should be trained in information security
The user doesn't understand the meaning of information security	The user should be involved from the beginning
The user is seen as security risk	The user should be accepted as partner in security questions

We postulate a cultural change in information security management: A socio-cultural, human centric approach that is based on trust and partnership, accompanied by appropriate security technology.

Trust can be circumscribed as: „One leaves others an opportunity to harm one when one trusts, and also shows one's confidence that they will not take it. Reasonable trust will require good grounds for such confidence in another's good will, or at least the absence of good grounds for expecting their ill will or indifference. Trust, then, on this first approximation, is accepted vulnerability to another's possible but not expected ill will (or lack of good will) toward one" [Baier 1986]. In this definition we see two important points:

- The trustor accepts willingly the risk of ill will of a trustee.
- The trustor has confidence, that the trustee will not take this possibility.

We have to be aware that 100% security is not possible besides not being cost effective. In information security the costs of the countermeasures must always be compared with its benefit of decreased risk. Thus the same applies to technical countermeasures as to human measures: We have to accept some residual risk. The security policy has to define, how big this residual risk shall be.

Concerning trust, we can differ two types, a cognition-based and an effect-based type. The later is a social trust, "it encompasses care and concern, benevolence, altruism, a sense of personal obligation, commitment, mutual respect, openness, a capacity for listening and understanding, and a belief that sentiments are reciprocated" [Scott and Gable 1997, 108]. The first is a rational trust that can be actively build up by training and/or experience, "it encompasses competence, ability, responsibility, integrity, credibility, reliability, and dependability" [Scott and Gable 1997, 108]. Trust can have various directions: unidirectional, bi-directional and transitive. It can also involve different parties. In our trust model we define trust with regard to information security as cognition-based and bi-directional between an organization, its managers and owners respectively, and its employees. Trust can have some economic advantages: Economic theory suggests, that trust lowers the risk of a transaction and therefore also lowers transactional costs [Chircu, et al. 2000, 1]. How can an organization have confidence in their employees, that they don't misuse their trust (and vice versa)? How can an organization build up trust regarding information security? In the next section we show a possible way to build up this trust.

4. INFORMATION SECURITY CULTURE

Corporate culture defines, how an employee sees the organization [Ulich 2001, 503]. In organizational theory a minimum of two opposite assumptions on corporate culture can be identified [Schreyögg 1999, 438], [Rühli 1991, 14]. In the functionalistic view, corporate culture influences the behaviour of its organizational members: Every organization *has* its own culture. In the opposite, cognitive-interpretative view, the theory of corporate culture is used to explain the organization's phenomena of a mini society: Every organization *is* a culture. In our paper we follow the theory of [Rühli 1991], that these two approaches can be integrated. The corporate culture is therefore a collective phenomenon that is growing and changing over time *and* it can be influenced or even designed by the management of the organization.

The core substances of the corporate culture are basic assumptions and beliefs. These assumptions concern the nature of the people, their behaviour and their relationship. The corporate 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. They are expressed in form of artifacts and creations such as handbooks, rituals and anecdotes. Ultimately the corporate culture has a crucial impact onto the corporate success [Rühli 1991, 15]. Corporate culture emerges and grows with time. It is formed by the behaviour of dominant organization members like founders and top managers. The three layers of security culture and their interactions are illustrated in *Figure 2.*

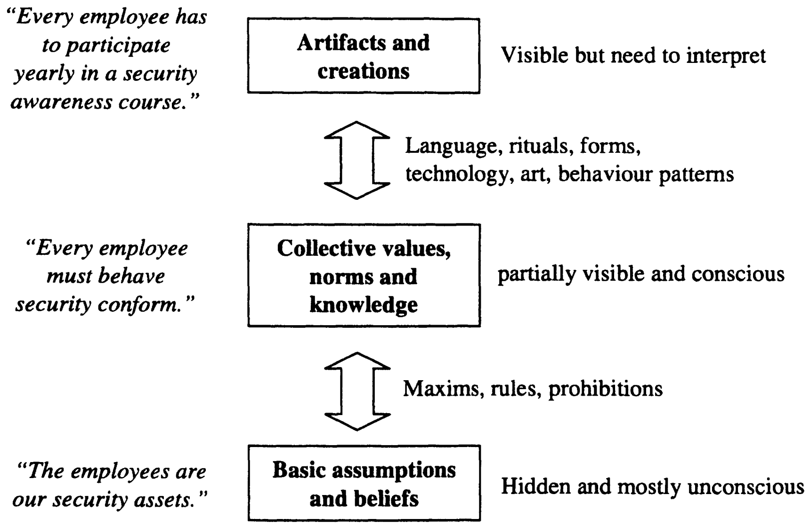

Figure 2. The three layers of security culture and their interactions [Schein 1985, 14] with examples for information security culture

A corporate culture can have different subcultures based on sub-organizations or content. The subculture is a subsystem that has specific values, norms and knowledge, which differentiates it from the corporate culture. An organizational subculture could be the values, norms and knowledge of the informatics or of the sales department, whereas the information security culture is a subculture in regards to content. Security culture should support all activities in a way, that information security becomes a natural aspect in the daily activities of every employee. Corporate culture helps to build the necessary trust between the different partners in our trust model. According to [von Solms 2000, 616], the security culture is addressing the "my own user is my biggest enemy" syndrome.

The information security culture focuses on the socio-cultural aspects of information security management. To build up an information security culture, we can get inspired by the international nuclear safety advisory group [Brandao 1994]. After the catastrophe of Chernobyl, they defined the concept of the safety culture [International Nuclear Safety Advisory Group 1986], see also [Freitag 1994, 132]. With little modifications this safety culture can be adapted to the information security culture. The measures of the safety culture mainly target the layer of norms, values and knowledge.

According to this model, the security culture should define three layers of responsibility (see *Figure 3*):

1. Corporate politics
2. Management
3. Individuals

These layers are enclosed by the external basic conditions as well as the social norms and values that for example are expressed in national and international law.

On the corporate politics level, information security should be defined as a corporate target. This means that the top management is responsible to define the security policy. Consequently they must provide sufficient resources to implement this policy. This task could be delegated, e.g. to a chief security officer (CSO), but the top management as whole remains responsible. A CSO can be positioned on several places within the organization chart: in the informatics department, in a new staff unit or in an existing security department.

The different department managers are then responsible for the compliance of the information security policy and for the implementation in their units. They must be sufficiently motivated to observe the security policy; since without their assistance it's not possible to implement such a policy. To implement this security policy, the management must define and control the different security measures. Additionally they must qualify and train their employees. Security conform behaviour must be awarded, malicious security breaches prosecuted. Also, the security strategy must be audited and benchmarked on a regular basis.

On the individual layer, every employee must contribute to the security of the organization him/herself. He/she has to have a critical attitude, by asking:

- Have I understood my task?

- What are my responsibilities?
- In which relationship do they stand to the information security?
- Do I have enough knowledge to fulfil my task?
- Do I need help?

He/she has to act carefully and with due diligence. Abnormal behaviour of people or computer systems including malfunctions must be registered and reported. Furthermore, the user has to be integrated in the risk analysis process and the company should install an employee suggestion system.

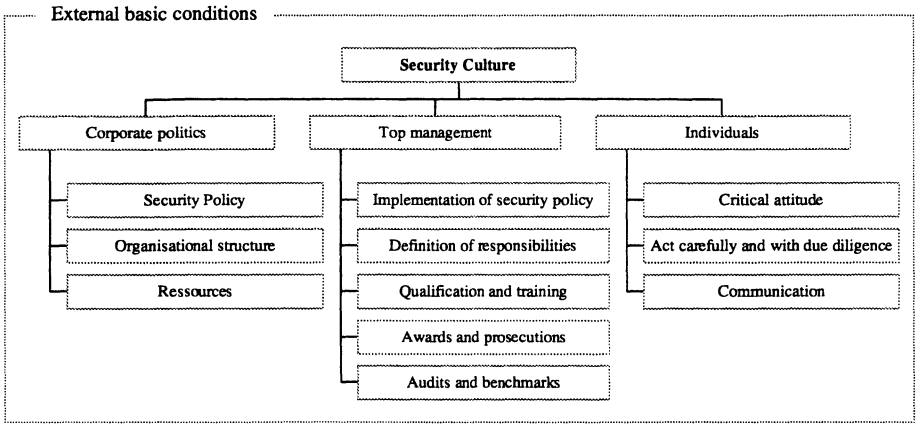

Figure 3. The layers of security culture

Concerning security culture the most important points are:

- The exemplary behaviour of the managers
- Security training of the employees, this includes creating awareness about the risks of information technology and training in the use of security products
- Awarding of security conform behaviour

It is important to notice, that security conform behaviour can also include making and confessing security breaches. Informing the management about errors and mistakes can help the organization to improve the security behaviour by better understanding the possible risks and errors. Only malicious behaviour should be prosecuted.

5. CONCLUSION

Humans and technology have different peculiarities, which are presented in the following *Table 2*. Humans can establish order in self-organizing form, whereas technology can only be used to sustain order using well-defined rules. The human being is a creative problem solver, whereas technology is dumb and deterministic. The strengths of humans and technology are thus complementary parts that can solve tasks together, which, individually approached, would be unsolvable.

Table 2. Difference peculiarities of humans and technology [Zumbach and Bilhuber 2001, 82]

Humans	Technology
Bundle of potentials - Humans "are" not, they "become" permanent - dynamic - adaptive	Bundle of attributes - technology "is" - deterministic
Combination of sense organs - orientation in complex, unexpected situations	Sensors - none to human comparable sense organs
Capable of anticipation	

Designing a security process and implementing a security technology should start at the business process and the employees working in this process, not at the technology. The combination of technology and human awareness and qualification can improve the overall security level of an organization greatly. In the words of the Oxygen project [Laboratory for Computer Science (LCS) 2001] – here used in a different context - security should become as natural as air. To reach this target it is necessary to have a security culture that addresses the socio-cultural aspects of security. We have shown the concept of security culture and we proposed also a way to implement this culture. There are still many open questions in this field, but information security can only be increased by the help of the users.

6. BIBLIOGRAPHY

Adams A. and Sasse M. A., "Users are not the enemy," *Communications of the ACM*, vol. 42 (12), pp. 41 - 46, 1999.

Attack Registry & Intelligence Service (ARIS), "ARIS Analyzer," SecurityFocus, 2001, http://aris.securityfocus.com, accessed on 23.10.2001.

Baier A., "Trust and antitrust," *Ethics*, 1986.

Brandao R., "IT-Sicherheitskultur im Unternehmen," diploma thesis *IFI*. Zürich: Universität Zürich, 1994, pp. 110.

Chircu A. M., Davis G. B., and Kauffman R. J., "Trust, Expertise and E-Commerce Intermediary Adoption," presented at The 2000 Americas Conference on Information Systems, Long Beach, CA (USA), 2000.

Computer Security Institute, "2001 CSI/FBI Computer Crime and Security Survey," *Computer Security Issue & Trends*, vol. 7 (1), pp. 1 - 20, 2001.

Freitag M., "Sicherheitskultur (Safety Culture) - ein brauchbares Konzept für Systemsicherheit und Arbeitssicherheit?," in *Psychologie der Arbeitssicherheit*, Burkhardt F. and Winklmeier C., Eds. Heidelberg: Roland Asanger Verlag, 1994.

Furnell S. M., Dowland P. S., Illingworth H. M., and Reynolds P. L., "Authentication and Supervision: A Survey of User Attitudes," *Computers & Security*, vol. 19 (6), pp. 529 - 539, 2000.

Gerbich S., "IT-Security 2001: Sind sie (noch ganz) dicht?," *Informationweek* (18), 2001.

International Nuclear Safety Advisory Group, "Summary Report on the Post-Accident Review Meeting on the Chernobyl accident," *Safety Series*, vol. 75-INSAG-1, 1986.

Laboratory for Computer Science (LCS), "MIT Project Oxygen," MIT, Laboratory for Computer Science, 2001, http://www.oxygen.lcs.mit.edu, accessed on 23.10.2001.

Rühli E., "Unternehmungskultur - Konzepte und Methoden," in *Kulturmanagement in schweizerischen Unternehmungen*, Rühli E. and Keller A., Eds. Bern / Stuttgart: Verlag Paul Haupt, pp. 9 - 48, 1991.

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

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

Scott J. E. and Gable G., "Goal congruence, trust, and organizational culture: strengthening knowledge links," presented at The eighteenth international conference on Information systems, 1997.

Ulich E., *Arbeitspsychologie*. Zürich: vdf, Hochschulverlag an der ETH Zürich, 2001.

von Solms B., "Information Security - The Third Wave," *Computers & Security*, vol. 19 (7), pp. 615 - 620, 2000.

Zumbach F. and Bilhuber E., "HRM im Spannungsfeld zwischen Mensch, Technik und Organisation," in *Excellence durch Personal- und Organisationskompetenz*, Thom N. and Zaugg R. J., Eds. Bern: Paul Haupt Verlag, 2001.