TOOL SUPPORTED MANAGEMENT OF INFORMATION SECURITY CULTURE

Application in a Private Bank

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

Abstract: In this paper, we present a management process we have developed for an Information Security Culture. It is based theoretically on action research and practically on expert interviews and group discussions. A Decision Support System, which supports the process, allows quick survey of the existing Information Security Culture in an organization and analysis of the results, thus discovering strong and weak points. This tool recommends, based on stored measures and rules, actions to improve the weak points. It helps security officers to do their work and to improve the Information Security Culture in their organizations. The application of the process and the Decision Support System in a Private Bank is presented here and major findings are discussed.

Key words: Information Security; Information Security Culture; Awareness; Assessment; Decision Support System.

1. INTRODUCTION

The intensified dependence on information processing in recent years has increased the organizational risk of becoming a victim of computer abuse. This risk will continue to rise within the coming years. Existing technical and procedural countermeasures can be enhanced by socio-cultural measures to increase the security awareness and the security knowledge of staff within an organisation, thus improving the security level of the whole organization (Martins, Eloff 2002; Schlienger, Teufel 2002). Potential losses by cyber attacks, computer abuse and industrial espionage can be prevented. Security culture should support all activities in such a way that information security becomes a natural aspect of the daily activities of every employee. It can

help to build the necessary trust between the different actors and should become part of the organizational culture, which defines how an employee sees the organization (Ulich 2001: 503). It is a collective phenomenon that grows and changes over time and can, to some extent, be influenced or even designed by the management.

This paper discusses first our management process for analyzing, maintaining and changing Information Security Culture. We then present a Decision Support System that supports this management process. This tool is designed to quickly analyze the existing culture and to automatically propose measures to improve weaknesses. It also allows comparison of the Information Security Cultures between different organizations (benchmarking) or that of a Culture within the same organization over different points in time. In this instance, the management process and tool were applied in a project at a Private Bank. We discuss the settings and findings of this project and the lessons learned.

2. MANAGEMENT OF INFORMATION SECURITY CULTURE

Information Security Culture, like organizational culture, cannot be created once and then used indefinitely without further action or modification. To ensure that it corresponds with the targets of an organization, culture must be maintained or modified continuously. It is a never ending process, a cycle of analysis and change. The first step is to analyze the actual Information Security Culture (diagnosis). If the culture does not fit with the organization's targets, the culture must be changed. If it fits, it should be reinforced. The necessary actions must be chosen (planning) and realized (implementation). The success of the actions taken must then be checked and learning specified (evaluation). The process is illustrated in Figure 1.

2.1 Process Description

In the following section, we give a short overview of these four management steps.

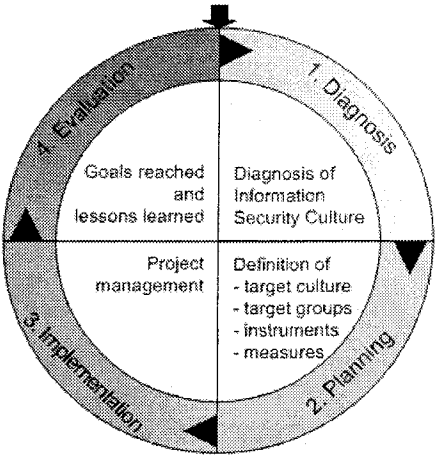

Figure 1. Information Security Culture management process

2.1.1 Diagnosis

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 its study. Bearing in mind the difficulties in comprehending culture at all, the use of a combination of measurement tools and methods as proposed among others by (Rühli 1991; Schreyögg 1999) seems evident. This allows verification of the results with other methods and the use of different viewpoints in interpreting them. The researcher is thus able to pick the appropriate methods, which help him/her assess the security culture in his/her organization. In our research we use:

- Analysis of security specific documents, e.g. security policy
- Questionnaires with employees
- Interviews or questionnaires with security officers
- Observation, e.g. clean desk policy verification

A more detailed discussion of the evaluation items and methods can be found in (Schlienger, Teufel 2003). In this paper, we concentrate only on questionnaires, as they are the instruments best suited for a tool supported assessment. We have developed a standardized questionnaire on the basis of the organizational behavior model of (Robbins 2001), see also (Martins, Eloff 2002). This divides organizational behavior into three layers: organization, group and individual, with in all twenty areas (e.g. work and technology design, communication, attitude etc.). The questionnaire has 42 questions, which are answered on a five point Likert scale from 1 (I strongly agree) to 5 (I strongly disagree).

2.1.2 Planning

The diagnosis step reveals the actual culture and its weaknesses. Depending on the target culture, specific actions must be taken to maintain or even change the culture. It is important to bear in mind that changing an existing, inappropriate culture needs more radical measures than maintaining an appropriate culture. Whereas an appropriate security culture can be maintained by an effective awareness programme, changing a culture involves the reengineering of all existing cultural measures.

Clear objectives for the development of an appropriate security culture must be set. We propose using the security policy as a definition of the target security culture. It is an overarching document for all measures concerning information security and defines the basics for security behaviour, see also (von Solms, von Solms 2004). To be able to define the right cultural measures, it is also essential to know which people one wishes to influence. A widely used approach is to define three groups: IT-staff, managers and lower-level employees/support staff, and to implement special measures for each group. In our research, segmentation by function (IT vs. business) or hierarchical position (managers vs. lower-level employees/support staff) revealed statistically significant differences that suggest the need to define special cultural measures for specific departments or management levels.

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. A number of possible instruments exist to influence Information Security Culture, the most important ones are: responsibilities, internal communication (awareness campaigns), training, education and exemplary action of managers.

2.1.3 Implementation

The planned actions must now be implemented. This phase can be organized as for every other project: it is essential to define detailed activities, responsibilities and resources, the schedule and the budget. We will not go into details concerning this phase.

2.1.4 Evaluation

Evaluation is the last step in our Information Security Management process. It provides valuable information about the efficiency and effectiveness of the actions implemented. It helps to improve the actions taken, to define necessary follow-up and also to legitimate investment in

Information Security Culture. This is especially important in applying for the following year's budget.

To highlight the changes achieved in a culture, the same instruments, in our case the same questionnaire, should be used. This questionnaire can be complemented by specific questions on the actions taken to reveal its effectiveness. Evaluation also reinforces organizational learning (Argyris, Schon 1978):

1. single loop learning ("adaptation"): the actions taken are evaluated to be improved in the future, e.g. the educational programme can be improved, knowing the strengths and weaknesses.
2. double loop learning ("change"): the evaluation also has an impact on the Information Security Culture itself. Undertaking an evaluation affirms the importance of information security. Employees pay attention to this topic once again.
3. deutero learning ("learn how to learn"): evaluation also helps to improve the evaluation process itself. Experiences from carrying out an evaluation will change and improve further evaluations of Information Security Culture.

2.2 Scientific and Practical Foundation

The proposed management cycle has its roots in a scientific research method and in practical exchange of ideas and experience.

The scientific root lies in action research. It is an established research method, used in social sciences since the mid-twentieth century, and it gained much interest in information systems research toward the end of the 1990s (Baskerville 1999; Björck 2001; O'Brien 2001). Action researchers assume that complex social systems, like an organization and its information systems, cannot be reduced to components for meaningful study. They can be best studied by introducing changes in social processes and then observing the effects of these changes. This involves five steps: diagnosis, action planning, action taking, evaluating and specifying learning. In our management process we use the same steps, but have integrated the steps evaluation and learning, since learning normally accompanies all steps but is most important in the evaluation.

The process has also been checked concerning practicability during discussions within the Working Group "Information Security Culture" of the FGSec (information security society Switzerland). The group consists of nine researchers, security officers and security consultants with experience in socio-cultural measures in information security. The process has been proved practical in this expert round and is now the recommended procedure of managing Information Security Culture.

3. A DECISION SUPPORT SYSTEM FOR THE MANAGEMENT OF INFORMATION SECURITY CULTURE

The complexity and the interdependence of information systems and of information security management are steadily growing. Providing tool support to security officers helps them to cope with complex decision making under time pressure. Computer based tools impart knowledge, which can provide the necessary foundation for decisions. Information systems that help to analyze the existing culture and to propose possible actions for improving weaknesses can be a major asset for the information security officer. The problem field of Information Security Culture management is either not structured, or, at the least, badly structured, and therefore not suited to automated decision taking. It is therefore not possible to build complete decision trees with all actions and consequences. Although a tool for Information Security Culture management is therefore not a Decision Support System in its narrow sense, it is one in a broad sense.

Decision Support Systems are not decision automatons, but they can help the user to prepare for decision making by surveying, filtering, completing and aggregating information. Decision Support Systems help to (Hättenschwiler, Gachet 2003):

- make decisions faster,
- improve the quality of decisions,
- reach the goals with fewer resources and
- make more rationale, robust and replicable decisions.

The tool supports in its first stage, see also (Krieger 2004), the management of Information Security Culture in the steps of diagnosis, planning and evaluation. The architecture is illustrated in Figure 2. It surveys the Information Security Culture with two questionnaires, one for all staff (survey component A) and one for the security officer (survey component B). It automatically analyzes statistically the survey results, discovers weaknesses in the culture and proposes actions to improve weak points (reporting component). Thus the security officer quickly obtains status information and knowledge about the Information Security Culture of his/her organization. He/she can then choose actions from the proposition list and implement them. The survey component can also be used to carry out the evaluation. An administration component allows administrators and researchers to manage surveys, questionnaires, best practices and users.

In a second stage further functions are planned. It is planned to support benchmarking survey results relating to one company with those of other companies and to improve the planning stage.

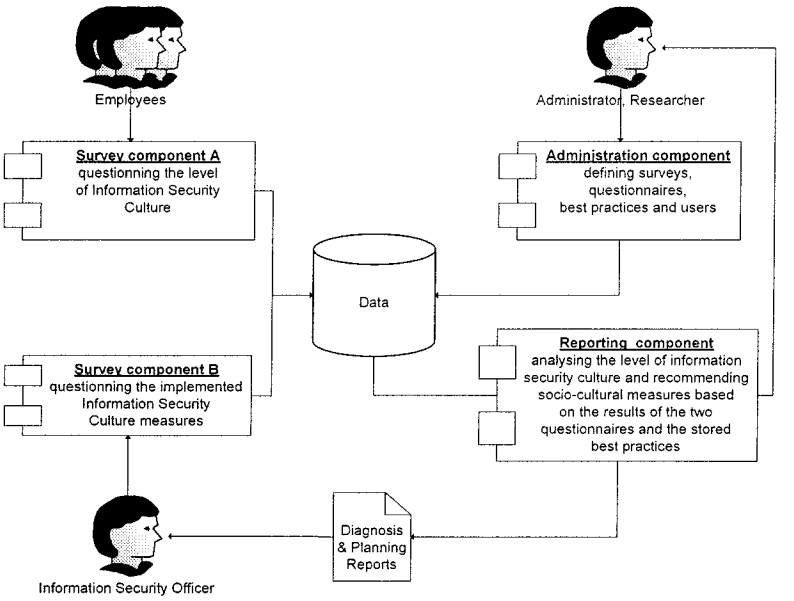

Figure 2. Architecture of the Information Security Culture Decision Support System

The tool has been developed on the web technology html and ASP.NET; results are stored in the free runtime version of Microsoft SQL server, and the analysis and reporting is undertaken with Crystal Reports. The web based client/server technology allows easy distribution of the application.

4. DEMONSTRATION AND CASE STUDY: APPLICATION TO A PRIVATE BANK

The tool was applied in a Private Bank in November 2004. Whereas the bank has employees worldwide, most of the staff works in Switzerland. The company has already carried out an information security awareness programme this year and is now starting to analyze its Information Security Culture in a systematic way. The project was supported by the top-level management and was signed by the CEO, CFO, COO, Head of Enterprise Risk and Head of Information Security. The project was thus backed by the highest hierarchical levels.

4.1 Diagnosis

We first discuss the survey setting with the online questionnaires. Then we present the reporting function of our Decision Support System, which displays the results of the survey but also findings and propositions to improve weak points in the Information Security Culture. The reporting component therefore covers the diagnosis and planning steps.

4.1.1 Survey

A questionnaire to survey the culture, in English and German, was prepared on the server of our Institute. Internet connection was secured with SSL. We used the standardized questionnaire, but dropped two questions that are not relevant for the organization and added six new questions. Although we always recommend and propose using the standardized questionnaire, it is frequently necessary to adapt it to the specific needs of an organization. Comparability between organizations is still given on the area level, where several questions concerning a specific area are aggregated.

The employees were invited by an email from the Head of Information Security to fill out the questionnaire. They also received the URL to the questionnaire with an anonymous company login and password. On the questionnaire, and prior to answering the questions, each employee first has to authenticate him-/herself and also to indicate his/her position (3 levels), his/her function (7 functions) and his/her region (4 regions). The questionnaire then consists of 46 mandatory questions and a section for optional comments. Cookies are set to anticipate multiple answers from the same account.

The Head of Information Security answered the security officer's questionnaire, which surveys the measures already taken to create and support an appropriate Information Security Culture. The database currently stores 87 answers from other security officers of Swiss organizations. Comparing an organisation's results with those of other Swiss organizations gives valuable information about the maturity of the Information Security Culture from the security officer's viewpoint.

Approximately 19% of all staff in Switzerland and Liechtenstein responded to the survey. The confidence interval of 7.36 at a confidence level of 95% provides enough accuracy for a statistical analysis of this group. However the feedback of only 0% to 5.5% from the other three regions gives us not enough data for a statistical analysis of these branches. One main problem of the two branches in Asia was the poor Internet access. In spite of that, the general problem of all three branches apparently is the lack of interest in information security.

4.1.2 Reporting

The reporting section is designed for the security officer and the senior management. It shows the answers on different aggregation layers:

- Overview: all questions aggregated, to give an overall picture (see Figure 3).
- Level: the questions concerning Organization, Group and Individual are aggregated to give level information.
- Area: the questions concerning an area are aggregated to give a more detailed picture of the areas. This analysis is called the Information Security Culture Radar and gives a wide range of information at a glance. It is the favourite aggregation level for benchmarking (see Figure 4).
- Single question: the results of a single question give the most detailed information.

The results can be filtered according to position, department and region to receive more details and to be able to define specific actions for target group. The report can be exported to different formats (PDF, Word and Html). Figure 3 shows the navigation of the reporting component and the entry screen with the overview. On the left side is a navigation tree, where the user can jump directly to the different levels, areas or questions. On the top are the filters and also the export function. The second top line offers

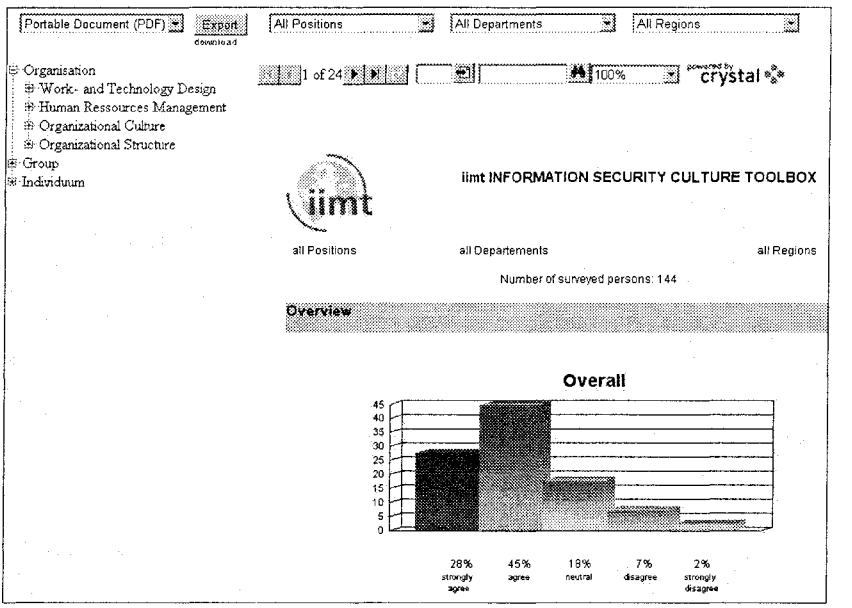

Figure 3. Overall results and Navigation

possibilities for searching and navigating through the pages.

The overall result (Figure 3) of 73% agreement is good. In discussion with the working group, we set the threshold for a satisfactory Information Security Culture at 60% agreement for each question. This number can be adjusted by the organisation for each question if wanted. In our survey the CSO agreed to the recommended threshold. Although the overall result is good, the analysis of areas and individual questions reveals improvement points.

The Information Security Culture Radar (Figure 4) shows the results on the area aggregation layer. It shows at once where the strengths and weaknesses are. Weaknesses are on the areas Human Resources Management, Organisational Culture and Problem Management. Actions should focus on improving the worst areas and maintaining the good areas at the same level.

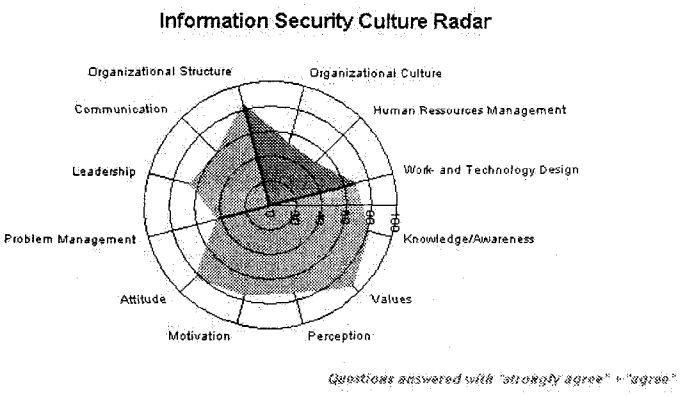

Figure 4. Area results: the Information Security Culture Radar

4.2 Planning

The reporting function also covers some of the planning phase. Its function is to automatically discover weaknesses and to propose improvement actions, based on rules and actions stored in the database. These actions are based on the results of the expert group. If a single question receives less than the agreement threshold, improvement actions are proposed. Filtering on position, department and region allows checking on whether the actions have to be implemented for everybody or for specific target groups.

The Decision Support System helps the security officer to quickly spot weaknesses and to retrieve possible measures. Depending on the specific

situation and specific needs, he or she can then choose preferred actions and implement them in his or her organization.

Figure 5 shows the result of the question "I receive training (courses, presentations, self-study etc.) in security applications and procedures I need for my work." The threshold is not reached, so the system reveals a problem and proposes improvement actions. In this case, employees do not receive the necessary information security training. The proposed measures focus on general information security education and specialised training in security procedures and tools.

4.3 Future steps: Implementation and Evaluation

The bank is going to implement the most promising improvement measures during 2005. It is also planned to evaluate the actions taken in an evaluation survey at the end of 2005 or beginning of 2006. The evaluation step is necessary to a systematic management of Information Security Culture. It gives valuable information about the effectiveness and efficiency of the implemented measures and supports organizational learning.

We expect valuable improvement of information security in this bank and hope that systematically managing Information Security Culture will become a part of its organizational culture.

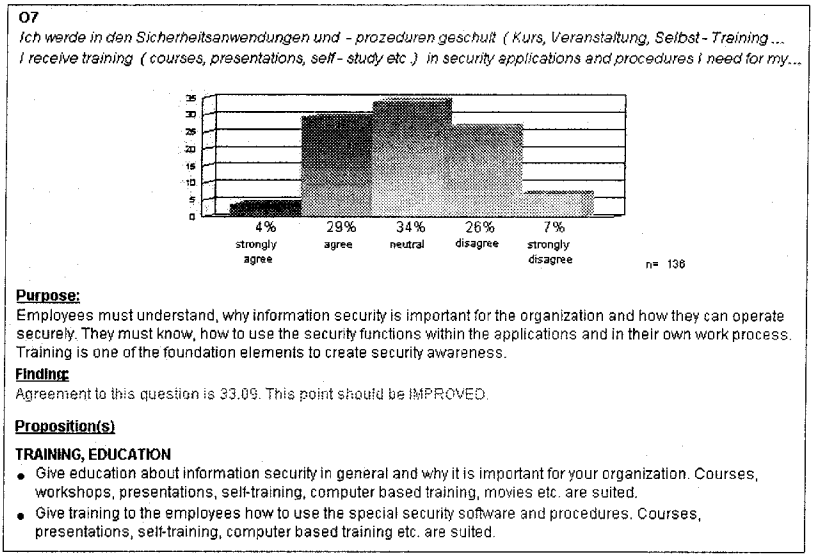

Figure 5. Question results with problem description and improvement propositions

5. CONCLUSIONS

In our survey on Information Security Culture in Swiss Organizations (Schlienger, Rues Rizza 2004) we discovered that most of the organizations rate the socio-cultural dimension of information security as very important. However, they encounter problems in proving its value in terms of improvement in information security and return on investment. The proposed method and tool helps to bridge this gap by allowing organizations to systematically analyze their information security culture, to quickly identify weaknesses and improvement actions and to prove progress in Information Security Culture. The application in a real world project shows its usefulness and the experience shows that we have reached our goals. In future development we will extend the functions of the Decision Support System to provide benchmarking and better support in the planning phase.

ACKNOWLEDGMENTS

We thank all members of the Working Group "Informationssicherheits-kultur" (Information Security Culture) of the FGSec (information security society Switzerland) for their valuable discussions and cooperation. We especially thank Stefan Burau for giving us the opportunity to apply the management process and the Decision Support System in practice and to gain valuable experience with it. The successful implementation of the first prototype of our Decision Support System is thanks to Manuel Krieger.

REFERENCES

Argyris, C. and D. A. Schon (1978). Organizational learning. Reading, Mass., Addison-Wesley Pub. Co.

Baskerville, R. L. (1999). Investigating Information Systems with Action research, Communications of the Association for Information Systems. Volume 2, Article 19. http://www.cis.gsu.edu/~rbaskerv/CAIS_2_19, 11.3.2004.

Björck, F. (2001). Security Scandinavian Style: Interpreting the Practice of Managing Information Security in Organisations. Licentiate Thesis. Department of Computer and Systems Sciences. Stockholm, Stockholm University & Royal Institute of Technology.

Hättenschwiler, P. and A. Gachet (2003). Skriptum in Decision Support Systems Theory I. University of Fribourg.

Krieger, M. (2004). Ein Decision Support System für das Management der Informationssicherheitskultur. Masterarbeit. Lehrstuhl für Management der Informations- und Kommunikationstechnologie, Universität Freiburg i.Ue.

Martins, A. and J. H. P. Eloff (2002). Information Security Culture. 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: 203-214.

O'Brien, R. (2001). Um exame da abordagem metodológica da pesquisa ação [An Overview of the Methodological Approach of Action Research]. In: R. Richardson, Ed. Teoria e Prática da Pesquisa Ação [Theory and Practice of Action Research]. João Pessoa, Brazil, Universidade Federal da Paraíba. English version: http://www.web.ca/~robrien/papers/arfinal.html (11.3.2004).

Robbins, S. P. (2001). Organizational Behavior. New Jersey, Prentice Hall.

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.

Schlienger, T. and R. Rues Rizza (2004). Befragung zur Informationssicherheitskultur in CH Organisationen, Arbeitsgruppe "Informationssicherheitskultur" der FGSec (information security society switzerland). www.fgsec.ch/ag/isk/Marktbefragung2p.pdf, 9.11.2004

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: 191-201.

Schlienger, T. and S. Teufel (2003). Analyzing Information Security Culture: Increasing Trust by an Appropriate Information Security Culture. Proceedings of the International Workshop on Trust and Privacy in Digital Business (TrustBus'03) in conjunction with 14th International Conference on Database and Expert Systems Applications (DEXA 2003), September 1-5 2003, Prague, Czech Republic, IEEE Computer Society.

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

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

von Solms, R. and B. von Solms (2004). "From policies to culture." Computers & Security **23**(2004): 275-279.