CBISA - a DSS for Analysing a Company's Information Security: A Tool for Decreasing Uncertainty.

This report is a preliminary version of a paper to be presented at: Information Processing and Management of Uncertainty in Knowledge-Based Systems. Granada. Spain. July 1996.

Thomas Finne
Åbo Akademi University, Institute for Advanced Management Systems Research (IAMSR), DataCity, Lemminkäisenkatu 14 A, 4:th floor
20520 Åbo, Finland
E-mail: tfinne@mail.abo.fi

Turku Centre for Computer Science
TUCS Technical Report No 29
June 1996
ISBN 951-650-790-5
ISSN 1239-1891

Abstract

An inadequate level of information security can lead to considerable economic losses for a company. Therefore information security has to be considered an important function in a company. Since information security (ISEC) is an important function in a company, it should be possible to construct a system to analyse it.

Computer support is increasingly used in decision-making. Decisions on information security should also be computer-supported. I have created a decision support system (DSS) for analysing a company's information security. The DSS I have named; Computer-Based Information Security Analysor (CBISA). I consider that a decision-maker can, supported by the CBISA, decrease the uncertainty in decisions on information security.

1. INTRODUCTION

When I participated in the work of improving a company's information security, I noticed that we would have had great benefit from computer support. I consider that it should be possible to use a Decision Support System (DSS) when analysing a company's information security. I have constructed such a DSS and named it Computer-Based Information Security Analysor[1]. Supported by the CBISA the decision maker/s should be able to make decisions that support better information security in the company.

In a perfect world there would not be any information security breaches. However, as we all know, there is nothing 100% secure; this fact we have to accept and live with. There are also risks that cannot be totally delimited. To some degree a company has to live with those risks, e.g., the personnel security in a company. There is always a degree of risk with the personnel. By controlling the personnel thoroughly the unique risk can be minimised. However, it may be that an otherwise very reliable employee is blackmailed into "leaking" sensitive information. An investor should always take into consideration that there is an immovable risk, e.g., the risk that a natural disaster will happen and negatively affects the stock market [3]. When dealing with its ISEC a company should always take into consideration that there is an immovable risk.

Decisions on information security are made under uncertainty. For example, we cannot put a probability on hackers attacking our system and succeeding. This fact must not deject us but we have to try to manage the ISEC risks. Information security is, as a problem area, unstructured. Unstructured areas can be managed with the help of Decision Support Systems (DSS).

The technology used in information processing is in itself of great economic value. The investment that a company makes in both soft- and hardware can be worth millions and

---

[1] CBISA©TFinne. 1995-

the company's operations depend heavily on that investment. The investment is often unprotected because in many companies information security is not adequately regarded as an important function. This is very odd as inadequate information security can result in very negative consequences and bring huge economic losses [6]. I participated in the project group that organised a security questionnaire that was sent in summer 1994 to 1800 Finnish companies and public services. Out of a total sum of 521 respondents 434 reported breaches in their information security. Those had experienced 3309 breaches in their information security during the last five years. The breaches brought an weighted average cost of Fmk 35 000 ($1≈Fmk4.5) [13]. A similar survey was conducted in England in year 1994, by NCC, dti and ICL [12]. A total of 832 respondents representing a wide cross-section of industry and sizes of organisation reported over 6200 breaches. Over £9000 as an average cost for every breach represents a notable sum of money for any organisation, especially if hit by several breaches.

By putting resources into information security it is possible to avoid expensive and dangerous breaches to a company’s information security. However, a company has to put a limit on what resources they can stake on information security and the resources should be directed to those factors in a company’s ISC that have the greatest impact on the company’s information security. In this context information security is very much a management problem. I think that it is of the utmost importance that the investment is made in those factors most of all affecting a company’s ISEC. In that way it is possible to build up and maintain an information security chain. However, no link in the information security chain must be left too weak. Information security is also a huge area containing the most varying issues. According to Wood [17] information security is an interdisciplinary field.

A company’s information assets have to be protected, however this is not an easy task since a company's information security can be compromised by many dangers. For example, water leakage in buildings is becoming more and more common and such leakage in a computer room can have disastrous effects. Also nature itself may be a factor e.g., a thunderstorm can disrupt the electricity supply and so seriously damage unprotected hardware [5]. With growing competition and stiffening demands on research & development, industrial espionage and sabotage are likely to become increasingly important factors in ISEC. A company's information security can also be damaged by accident, e.g. an employee who uses her own disks at work may cause a damaging virus attack on the company's data files. An employee that "lets the cat out of the bag" can damage a company badly and nullify the effect of good (and expensive) information security solutions. This can be done either unintentionally or intentionally.

In my research I have divided up a company’s ISEC into 12 modules and 79 submodules. This dividing up I have used as a basis for building my DSS for research purposes.

2. WHAT IS INFORMATION SECURITY ?

To clarify what information actually is and the importance of information I quote Smith "..Possession of accurate, up-to-date and comprehensive information is now the key to growth and success, when once it was perhaps the ability to manufacture, or harvest crops, or trade overseas...[14]". We are living in a period of time when information becomes increasingly valuable. Information also becomes very quickly outdated. For example, a database containing vital data about customers can soon become out-of-date if not regularly updated. Thus a company has to know what information that is most valuable and put the efforts in protecting that information.

As I have pointed out, ISEC is a very large area. Also the security in a company has many forms and variations, for example, investment security, production security, customer security, environment security and information security. They depend on each other and build up the company's total security. To distinguish between the many forms of security and information security is quite difficult. To make it a bit easier I stipulate the following:
When information is threatened, lost or misused, it is a question of information security.

What is an information security analysis? The answer is: We analyse a company's information security. Why do we analyse it ? We analyse it to show the status of the company's information security and thus provide the basis for improving its information security.

3. DECISION-MAKING UNDER UNCERTAINTY

In a product mix problem where we know the profit per unit and the level of production, we make our decision under certainty [15]. We assume that we know the future perfectly [1]. When only partial or imperfect information is available about a problem, two new categories of decision-making appear:

1. Decisions under risk
2. Decisions under uncertainty

In the category 'Decisions under risk' the degree of ignorance about the data is expressed in terms of a probability density function. This means that we have some knowledge of the problem, but we do not have perfect knowledge. Decision trees are very useful for handling decision problems under risk [1]. With a decision tree we can make a graphical representation of the decision problem. In a decision tree we combine probabilities with different economic outcomes. In a decision tree there are two types of nodes: a square representing a decision point and a circle that stands for a chance event [15]. We can build quite extensive trees with many decision points and chance events. Concerning decisions under uncertainty Austin et al. point out that the problem involved has a large number of components and a substantial amount of interaction between and among the components. Sometimes the problem under consideration involves a system that is so complex that managers do not well understand its structure [1]. Concerning data availability, certainty and uncertainty represent two extreme cases. Risk exists somewhere between them [15]. I consider that decisions on ISEC are made under uncertainty. For example, we cannot put a probability on hackers attacking our system and succeeding. Naturally we can, supported by the necessary equipment, register the number of attacks. However, I think that we cannot put a probability on an attack occurring and/or it succeeding; for that there is not enough actuarial data.

The decision maker has to decide about the investments in information security. The decisions on ISEC are made under uncertainty. A company should reach an adequate level of information security within the constraints that a company's budget provides. The subject information security is huge so that we have to make it computer-based to be able to treat it. The CBISA is a tool for decreasing the uncertainty in decisions on ISEC.

4. WHAT IS A DECISION SUPPORT SYSTEM ?

Klein and Methlie define DSS as "A computer information system that provides information in a given domain of application by means of analytical decision models and access to databases, in order to support a decision maker in making decisions effectively in complex and ill-structured (non-programmable) tasks [8]".[2] Klein et al. point also out that, inter alia, the preferences, judgements, intuition, experience of the decision-maker are essential, and that the solution must be achieved in limited time [9]. Information security is a complex task and the problems are unstructured. In information security the decision-maker's experience is of special importance since the area is so huge. The resources to put into ISEC are sparse and therefore some things (submodules) have to be preferred to others. To avoid economic losses the solutions to information security have to be achieved in a limited time. We have to remember that when carrying out an ISEC analysis we do it as group work and the time used is valuable for the company.

The problems with a company's ISEC cannot be solved "simply" by using a procedure or algorithm; the problems are much more sophisticated than that. There is no formula that we can prescribe for each company and the subject information security is very elusive. New threats emerge at a steady rate in a company's information security. We cannot, with a DSS, solve all problems in a company's information security but I am quite sure that it is possible to decrease the size of the problems. In the CBISA each submodule is treated separately as a problem. Nevertheless but as a link in the information security chain. Each submodule is linked to a database that I have created on ISEC.

I consider that decision support systems are very useful tools for supporting decisions. However, we have to remember that DSS's have also drawbacks. For example, merely by working with a DSS we cannot change the environment. Environments are changed by the human beings acting on them [8]. The result of the CBISA is meant to function as

[2] Here I want to point out that the CBISA, if we really go into questions of definition, belongs to a subgroup of DSS's; Knowledge-Based DSS's. It would be a KB-DSS because it is provided with a database.

a starting point and framework when improving the ISEC. The information security can only be improved by the human beings, not by the CBISA.

5. MAPPING OUT THE CBISA

Briefly I will clarify the main parts in the CBISA[3]. With 'module thinking' I have divided up a company's information security in almost 100 modules and submodules. Each submodule contains information on a specified part of a company's ISEC. The information we use as a basis when analysing the status of that specific submodule in the company. By carrying out a risk assessment (RA) we can assess the economic losses for each submodule. With the ISPA (Information Security Portfolio Approach) we can find those submodules that can bring the heaviest economic losses. During the analysis we can make notes. In my example (see page 4) I select number one (computer security) and the submodules appear on the screen. I can now freely select with what submodule to start. Let us say that I want to know more about back-up, I select 'back-up' by double clicking on the word (when navigating in the CBISA we can use both 'buttons' and 'scroll bars'). The 'information window' appears and now the information needed for the ISEC analysis is available to the user. The user of the CBISA wants to analyse and improve information security and therefore needs the knowledge presented.

The user gets the knowledge from the database, built with Access, which is linked to the system. Each submodule contains 1/3 to 2 A4 page/s of information. The information I have gathered from a large number of sources and consolidated it with my own knowledge in the subject. By using the scroll bar the user can read all the information and questions about that module. The submodule 'back-up' contains approximately one page of essential information on back-up.

It is also possible to make notes during the analysis. The notes can be made for every submodule. Further, the questions that I have developed and included into the database function as a basis for making the notes. Thus we can make decisions during the analysis and write them down.

It is possible to print out the notes and/or save them on a disk. The notes can then be used as a basis when taking the measures for improving the ISEC. The notes can be saved for use as a reference point in the next analysis. This means that an information security analysis can be made at regular intervals (see next page):

---

[3] The CBISA is built with Visual Basic/Windows (Microsoft Visual Basic Version 3.0) and Access/Windows (Microsoft Access Version 2.0).

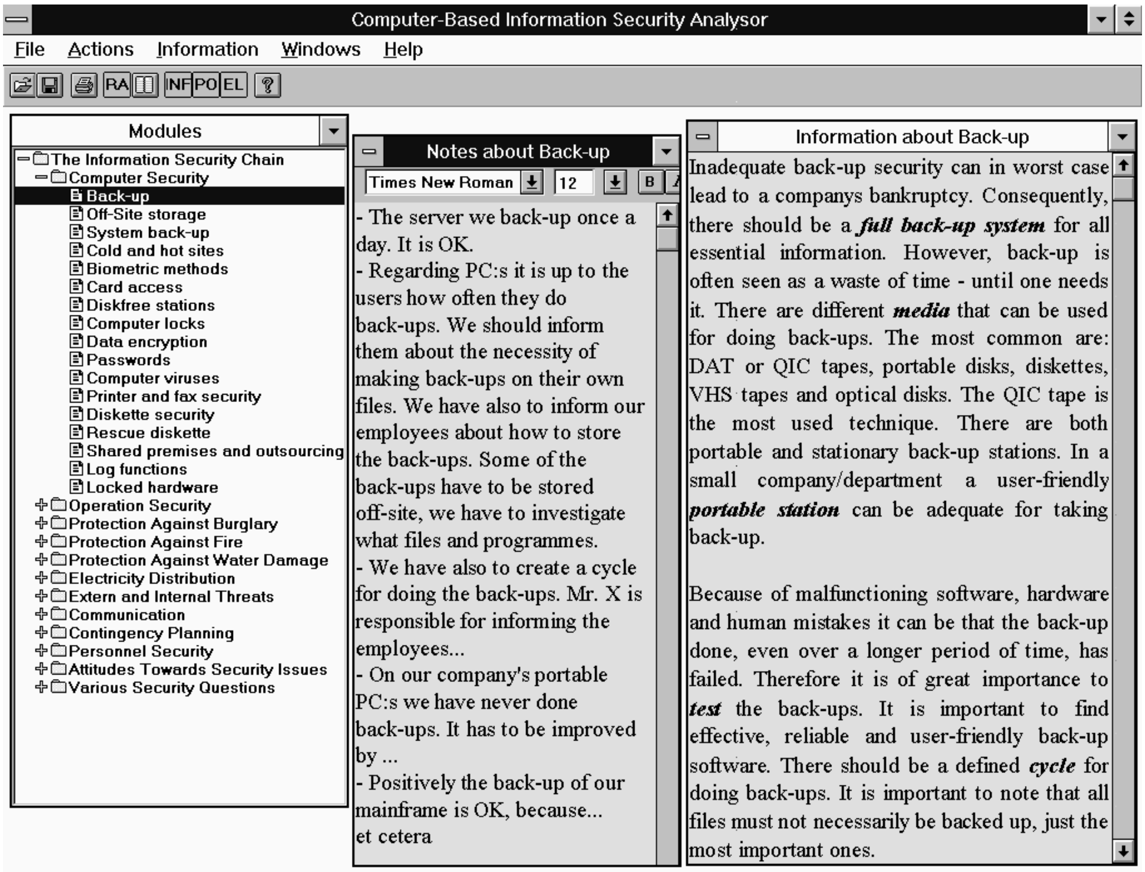

Figure 1: Using the CBISA

To go through the whole CBISA naturally takes some time. However, by systematically treating each submodule it is possible to carry out the analysis within a reasonable period of time. It is also noteworthy that the CBISA also can be used as a support tool when making a pilot study of the information security in the company. The CBISA functions also as a manual on information security.

We have now gained information about the submodule: back-up. The information is both qualitative and quantitative. We have also made notes about the submodule. As we want to carry out a risk assessment on this submodule, we push the ‘RA’ button. In the risk assessment we can put in the expected economic losses into different categories. More closely I have divided up the losses into the following categories:
Personnel resources, mental resources, image, production, hard & software, information lost, material and a company specific loss. I would say that the value of information is the most difficult to estimate.

According to Caelli et al. risk assessment is “an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level [4]”. We can use the CBISA’s ‘RA’ to compare expected losses with the investments needed. With the RA we should be able to get a rough assessment of the economic losses that we can be hit by, and in that way a basis for decisions on in what submodules to invest.

Zeleny uses the term “portfolio” with the expression “collection of assets” and “collection of prospects”. A portfolio can consist of bonds, shares, jewellery and investment ventures [18]. In a stock portfolio the risk normally diminishes strongly with the first 15-20 stocks included. When more stocks are included the benefit from the diversification gradually diminishes [3]. In an information security portfolio the factors should be included which have the strongest impact on information security. In this way a company would be able to spread the investment in ISEC in a sensible way and also get a good return on the investment (ROI). I have named my approach: ISPA (Information Security Portfolio Approach). The ISPA should not prevent us from investing in more than just the most important ones, but it is an unfortunate fact that most companies have limited resources to invest in information security. Smith proposes that the most important information security risks have to be dealt with first. When the company has been convinced, one can go for the more difficult tasks [14]. By identifying the most important factors we can convince the company about the importance of information security. Thus the approach provides us with two advantages: (i) that we can achieve an acceptable level of information security, and (ii) we can prepare the ground for further improvements. When we have carried out the risk assessment we can select from the scroll bar those 5, 10, 15, 20, 25 or 30 submodules that have brought the biggest expected losses. Let us say, to make it easy, that, after having performed the analysis, we select the 5 submodules with the highest expected losses. The ‘screen’ looks like the following:

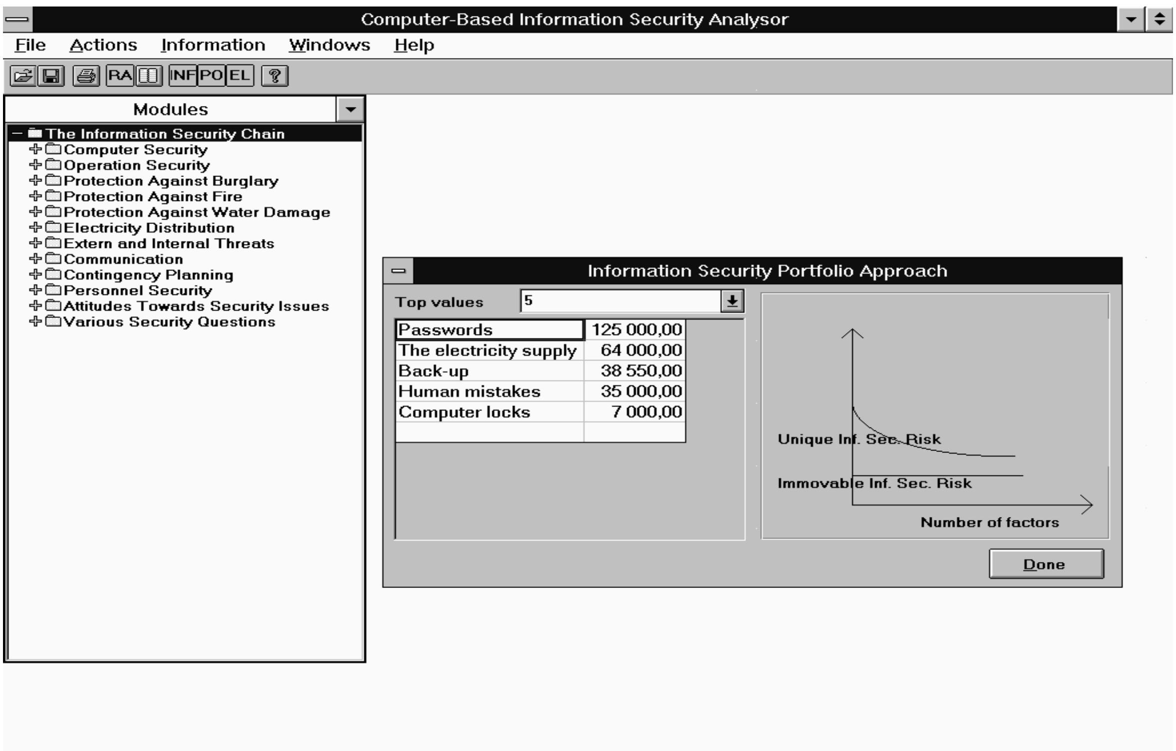

Figure 2: Information Security Portfolio Approach

6. USING THE CBISA - A CASE.

Company A1 is a unit in a multinational company. A1 has a turnover of approx. $200 million. When carrying out the analysis in the company-A1, I used a portable computer connected to an overhead projector and screen. By using a projector, each member of the project group[4] could follow the stages in the CBISA. I made all the notes and took part in the discussion. I think that the CBISA is nice to work with; the windows are easily movable so that many functions in the CBISA can be running simultaneously. The structure of the CBISA was very much appreciated by the project group. They considered that the dividing up had been done in a systematic way and by that the subject was treatable.

It was very much appreciated that the CBISA is more than "just" EDP. As usually pointed out their information security is much more than the computers.

The users were of the opinion that it is much better to have it computer-based than 'paper-based'. As one in the company considered: "Making the analysis on paper would have been very heavy". The analysis has to be carried out in co-operation with persons that thoroughly know the company. When carrying out the CBISA it is essential to have good support from the company. As it was pointed out [16] the role of management is crucial.

I consider that the CBISA is a tool for group work and (group) decision support. I think that the CBISA saves the company both time and money: time since it can be carried out in approximately three days, which is a quite small time when considering the nature of the subject; money because there are usually many expensive information security breaches in companies. The members in the project group considered that the time spent was a good investment because they can avoid time-consuming ISEC breaches in the future. The information security on the results of information security analysis has to be very high. According to Gallegos et al. [7], DSS techniques offer exceptional power, accompanied by some unique risks. One of the greatest risks associated with a DSS is the possibility of information leaks that would permit outsiders to assess the present state and characteristics of an organisation.

It would be very cumbersome to bear in the mind all the modules and submodules that the CBISA is built on. With the computer-based model it is possible to ease a decision-maker's burden. Quoting Bell et al. [2].: "Our decision makers are not economic automatons; they make mistakes, have remorse, suffer anxieties, and cannot make up their minds".

For further research I consider that scenario analysis could be implemented in the CBISA. This would be possible by implementing a 'notes for scenario analysis'. A project group could here even more freely 'brainstorm' around scenarios. For example, what would happen if the company were attacked by a computer virus ? Another place

[4] The project group contained 6 people (mostly managers) and represented a huge amount of knowledge about the company. Together we carried out the CBISA and made decisions.

for improvement was that there should have been more direct questions in the database. As one member of the project group pointed out, such questions could function as a more direct basis for discussions. Actually the questions were already in the text, but for further use in companies I separated them from the text. Further the user-friendliness would increase if the CBISA would be provided with graphics to show the result of the RA.

7. CONCLUDING REMARKS

Inadequate ISEC can bring heavy economic losses. The problems in information security are unstructured and I consider that they are best solved with the help of a DSS. I have built a DSS for information security. Supported by the CBISA the decision maker/s should be able to make decisions that support better information security. We cannot achieve 100% information security; however, our aim has to be to decrease the uncertainty. The CBISA is a tool for decreasing the uncertainty over decisions on information security. Perhaps in the future we will be able to put probabilities on, e.g., hackers attacking our computer system but today actuarial data on ISEC are too scarce for that.

The CBISA is usable as a support tool for making decisions in group. However, there is always a chief decision-maker who has overall responsibility. We have to remember that merely by using the CBISA we cannot improve the information security in a company; human beings have to carry out the improvements. Of great importance is that those persons that carry out the analysis are extremely reliable and follow strict personal information security. Also the results of the analysis have to be adequately protected.

Acknowledgements
Firstly I want to thank my supervisor, Professor Christer Carlsson at the Åbo Akademi University/IAMSR, for his invaluable support. Researcher Kim Johnsson at IAMSR has contributed with valuable expertise in the computerisation of the CBISA. A great thanks to him.

References

[1] *Austin, Larry M. & Parwiz Grandforoush.* Management Science for Decision Making. West Publishing Company. USA. 1993

[2] *Bell, D., H. Raiffa & Amos Tversky.* Decision Making Descriptive, Normative, and Prescriptive Interactions. Cambridge University Press. 1988

[3] *Brealey, R.A. & Stewart C.M.* Principles of Corporate Finance. McGraw-Hill. USA. 1991

[4] *Caelli, William, D. Longley & M. Shain.* Information Security for Managers. Stockton Press. UK. 1989

[5] *Finne, Thomas.* Information Security: An important function in a company, (Informations-säkerhet: en viktig funktion i ett företag). Forum för ekonomi och teknik. Number 8. 1994, pp 12-14, 24

[6] *Finne, Thomas.* Information Security: Vital for Competitive Advantages. Paper presented at the IFIP WG 11.1 Workshop. South Africa, Cape Town 8.5.1995

[7] *Gallegos, Frederick et al.* Audit and Control of Information Systems. Cincinnati. USA. 1987

[8] *Klein, Michel & Leif Methlie.* Expert Systems A Decision Support Approach.With Applications in Management and Finance. Addison-Wesley Publishing Company. Great Britain. 1990

[9] *Klein, Michel & Leif Methlie.* Knowledge-based Decision Support Systems with Applications in Business. John Wiley & Sons. Great Britain. 1995

[10] *Microsoft Corporation.* Visual Basic/Windows. Visual Basic Version 3.0

[11] *Microsoft Corporation.* Access/Windows. Access Version 2.0

[12] *NCC, dti, ICL.* IT Security Breaches Survey Summary. UK. 1994

[13] *Salonaho Mikael, ICL Data Oy, LAN Vision Oy.* Supervisor: Aimo Törn. Project group: Erkki Mustonen, Kari Laine, Timo Laine, Leena Meisalo, Marko Helenius, Thomas Finne, Petri Väänänen, Arto Ahti. Suomen tietoturvallisuutta käsittelevän kyselytutki-muksen tulokset. Finland. 1994. (Results from the Investigation on Information Security. Translated from the Finnish language by the author of this paper).

[14] *Smith, Martin.* Commonsense Computer Security, Your Practical Guide to Information Security. McGraw-Hill Book Company. London. 1993

[15] *Taha, Hamdy A.* Operations Research. An Introduction. MacMillan Publishing Company. New York. 1987

[16] *U.S. Department of Commerce/National Bureau of Standards.* Federal Information Processing Standards Publication. Guideline for Automatic Data Processing Risk Analysis. FIPS Pub. 1979 August 1

[17] *Wood, Charles C.* Effective Information Security Management. Elsevier Advanced Technology. Oxford. 1991

[18] *Zeleny, Milan.* Multiple Criteria Decision Making. McGraw-Hill Book Company. USA. 1982

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi/

University of Turku
• Department of Mathematical Sciences

Åbo Akademi University
• Department of Computer Science
• Institute for Advanced Management Systems Research

Turku School of Economics and Business Administration
• Institute of Information Systems Science