Computer Support for Information Security Analysis in a Small Business Environment.

This paper was presented at the IFIP WG 11.2. of TC11. Small Systems Security. Greece, Samos, 20:th of May 1996. Reprinted with permission.

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 30
June 1996
ISBN 951-650-791-3
ISSN 1239-1891

Abstract

Computer support is increasingly used in decision-making. Decisions on information security should also be computer-supported. I have created a prototype for a knowledge-based decision support system for analysing a company's information security. The KB-DSS I have named Computer-Based Information Security Analysor (CBISA). The CBISA I have used in a company for analysing its information security.

Key words: Computer-Based Information Security Analysor (CBISA), Knowledge-Based Decision Support Systems (KB-DSS), information security (ISEC), information security chain (ISC).

1. INFORMATION SECURITY - A FRAMEWORK

Numerous decisions are made daily in a company. Information plays an important part in decision-making. For a company a wrong decision can lead to drastic results; therefore information is steadily acquiring a more central role in business. Information must not be *wrong, manipulated or in other way useless*. A company's information assets have to be protected; however, this is not an easy assignment since a company's information security can be compromised by *many dangers*. For example; water leakage in buildings, interruptions in the electricity distribution, computer viruses, fraud, programming mistakes, failing hardware, inadequate back-up procedures, sabotage & espionage, fire and theft. 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. The mentioned improvement work was carried out in a medium-sized company in the retail trade. In my work in the company I used the *action research* methodology. Walden[1] describes action research as when: "the researcher not only studies social phenomena, but he/she participates in and actively influences the course of events". According to Arbnor[2] the action researcher works in the awareness that he changes the actors at the same time as the actors change him/her. It is a question of a mutual dialectical developmental process. I studied the literature and discussed with experts in the area. I presented my ideas to the company and received feed-back from the company. It was very much a question of a dialectical process where everyone gave knowledge - and received knowledge.

---

[1] Walden, Pirkko. Expert Systems in Strategic Market Management. 1992
[2] Arbnor, Ingeman et al. Företagsekonomisk metodlära. 1977

A very interesting result from the project was that I recognized the *information security chain (ISC).*[3] All factors affecting a company's ISEC build up an information security chain. The links in the ISC are key factors in a company's information security. In my research I have divided a company's ISEC into approx. 100 factors (modules & submodules) and made a computer-based tool for ISEC analysis. I have constructed such a KB-DSS and named it; *Computer-Based Information Security Analysor (CBISA)*[4]. Information security is, as a problem area, *unstructured.* As Klein et al[5] point out unstructured areas can be managed with the help of *Decision-Support Systems* (DSS). What is a KB-DSS ? It is a subgroup to DSS and following Klein et al's definition on KB-DSS "A KB-DSS can be defined as a computer information system that provides information and methodological knowledge (domain knowledge an decision methodology) by means of analytical decision models (systems and users), and access to data bases and knowledge bases to support a decision-maker in making decisions effectively in complex and ill-structured taks."[6] Why is the CBISA a KB-DSS ? Because it is a model provided with a knowledge base (database) to support the decision-maker.

Information security is a huge area containing the most varying issues. According to Wood[7] information security is an *interdisciplinary field.* As Smith points out it is of the utmost importance that the resources are invested in those factors that most affect a company's ISEC[8]. It is an unfortunate fact that a company has limited resources to invest in ISEC. Therefore the resources should be directed to those factors in a company's ISEC chain that have the greatest impact on the company's ISEC and that can bring the heaviest economic losses. However, *no link must be left too weak.* According to Murray[9] all resources should receive the appropriate protection, expensive measures should be reserved only for specific resources.

ISEC is an important function in a company, but is ISEC in itself profitable ? I would say that the profitability lies in the *avoidance of economic losses* that inadequate information security can bring a company. Losses of that kind are undoubtedly significant; however, actuarial data on such losses is scarce. A problem is also that it is very difficult to

---

[3] Finne, Thomas. Creating the Framework for an Information Security Analysis. 1995

[4] ©Thomas Finne. 1995

[5] Klein, Michel & Leif Methlie. Knowledge-based Decision Support Systems with Applications in Business. 1995

[6] Klein, Michel & Leif Methlie. Knowledge-based Decision Support Systems with Applications in Business. 1995

[7] Wood, Charles C. Effective Information Security Management. 1991

[8] Smith, Martin. Commonsense Computer Security, your practical guide to information security. 1993

[9] Murray, William H. Security should pay: It should not cost. 1995

calculate the economic losses that inadequate ISEC brings. For mapping out the ISEC in Finnish organisations, I participated in the project group that organised an information security questionnaire that was in summer 1994 sent to *1800 Finnish companies and public services*. The investigation contained a large number of questions. Out of a total sum of 521 respondents (298 companies and 223 public services) 434 reported breaches on their information security These had experienced 3309 breaches in their information security during the last five years. For 172 breaches the economic losses were reported; the average loss was Fmk 26200 ($ 1≈Fmk 4.5).

The feature of this paper is the CBISA and how it was to use in a company. The company where I carried out the analysis is a *unit* in a very big *multinational company*. The total number of employees in the unit is approximately 1000. The unit is heavily *computerised*, both in the office and in production. The unit has a turnover of almost *one billion Fmk*. The multinational company has many units in Finland and other parts of the world. The units in the company are quite *independent* from each other. I would say that some of them even compete against each other. The independence of the units has resulted in *differences* in their *IT*, i.e. there can be big differences between the make and type of software & hardware used by the units. The units employ independently most of their employees and not centrally through headquarters, which further increases their independence. The units' independence has resulted in there being *small systems* in the *big system* (multinational company). *Geographically* the units can be situated quite far from each other, which also makes them more independent.

2. CBISA - A KB-DSS for INFORMATION SECURITY ANALYSIS

I will clarify the *main parts* of the *CBISA*: With 'module thinking' I have divided a company's ISEC into *12 modules and 79 submodules*. Each *submodule* contains 1/3 - 2, A4 pages of *information & questions* on a *specified part* of a company's ISEC. This textbase of a total of forty A4 pages I have built on my own research results, working experience of ISEC and approx. 100 references on ISEC. This information we use as a basis when analysing the status of that specific submodule in the company. By carrying out *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*. This approach that I have created is based on Stock portfolio theory (see Brealey&Myers, Principles of Corporate Finance). During the *analysis* we can make *notes on every submodule*. The CBISA is built with *Visual*

Basic/Windows (Microsoft Visual Basic Version 3.0) and *Access*/Windows (Microsoft Access Version 2.0).

In accordance with good password security the CBISA is provided with a *password system*. There are two password levels, one level for the user and another level for the administrator:

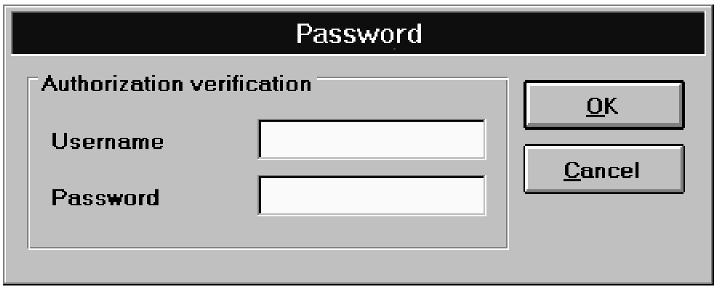

Figure.1: Password security in the CBISA

When the user has entered the password, the figure appears which explains the module thinking; this is the ‘logo’. From the figure it is possible to get an idea of the subject information security. The black square symbolises the company as it exists in the surrounding world. The *12* circles represent the modules that together form the information security in a company. Every module is situated partly on the outer side of the square. In this way I have tried to show that the surrounding world affects the information security in a company. Every module also includes many submodules with an influence on information security; this is symbolized by module number one. Thus the large circle represents the subject of information security which is made up of *12 modules and 79 submodules*

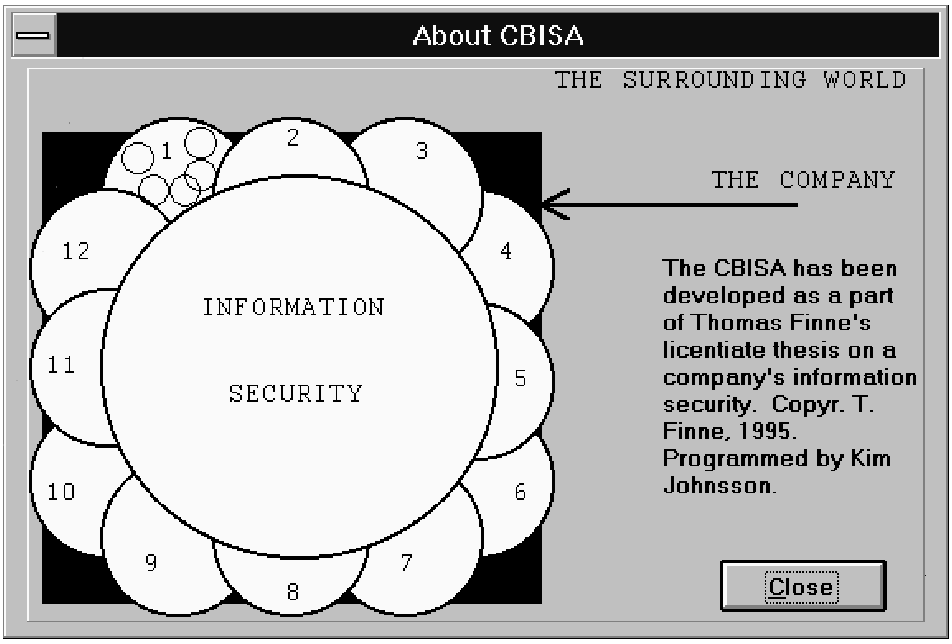

Figure.2: “Logo” in the CBISA

In the next step the *information security chain is represented* (all the modules and submodules). We can now *select* from the scroll bar the module and submodule with which we want to start the ISEC analysis.

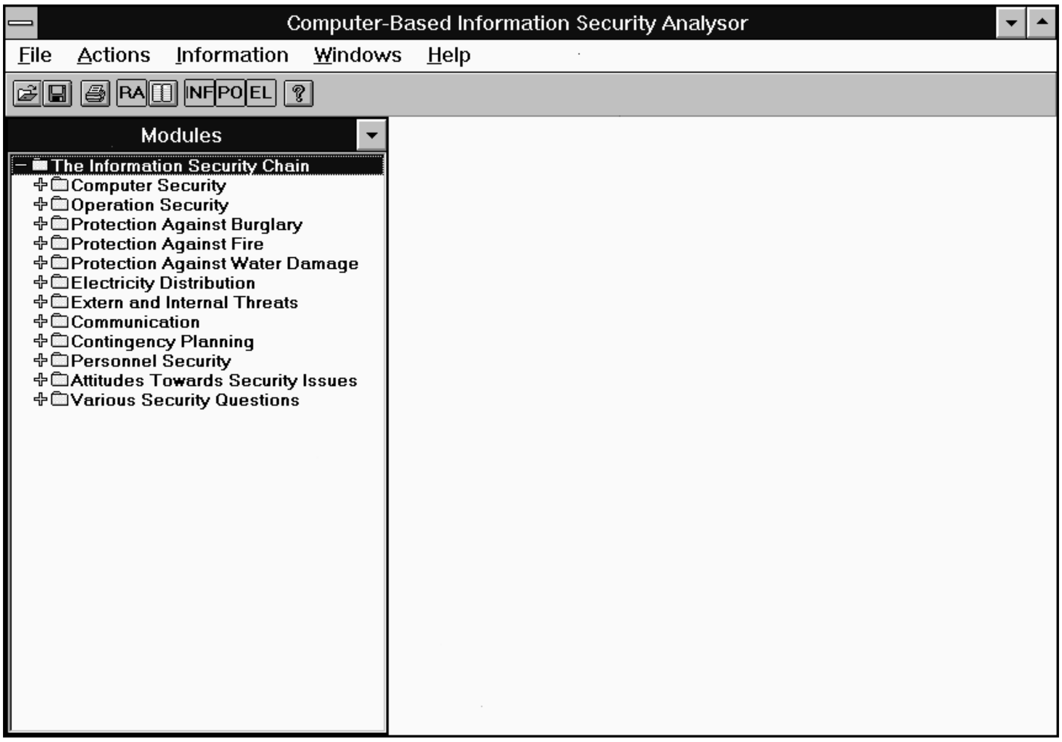

Figure.3: The information security chain

In this example I select the *first module* (computer security) and the *submodules* appear on the screen. I can now *freely* select with what submodule to start.

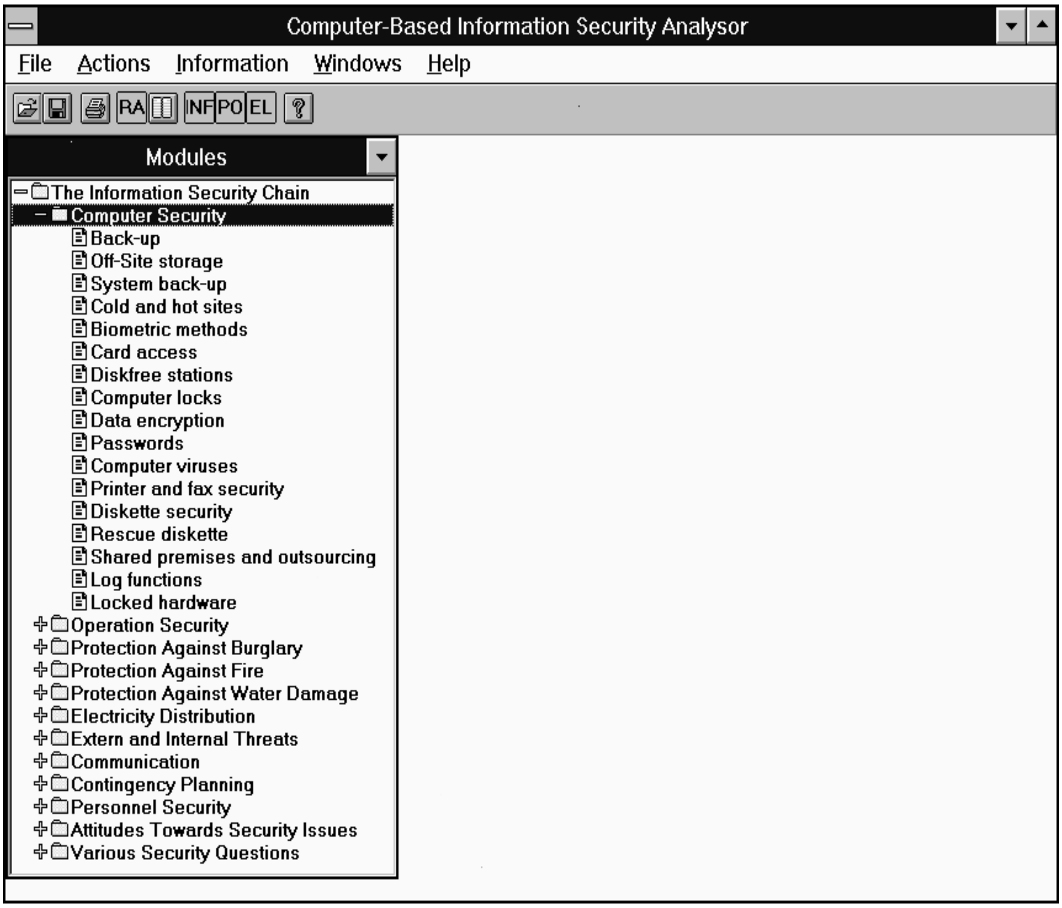

Figure.4: Choosing module

Let us say that I want to know more about *passwords*, I select ‘passwords’ 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 *knowledge* the user gets from the *database*, built with Access, which is linked to the system. By using the *scroll bar* the user can read all the information about that module. The submodule ‘passwords’ contains approximately two pages of essential information on passwords.

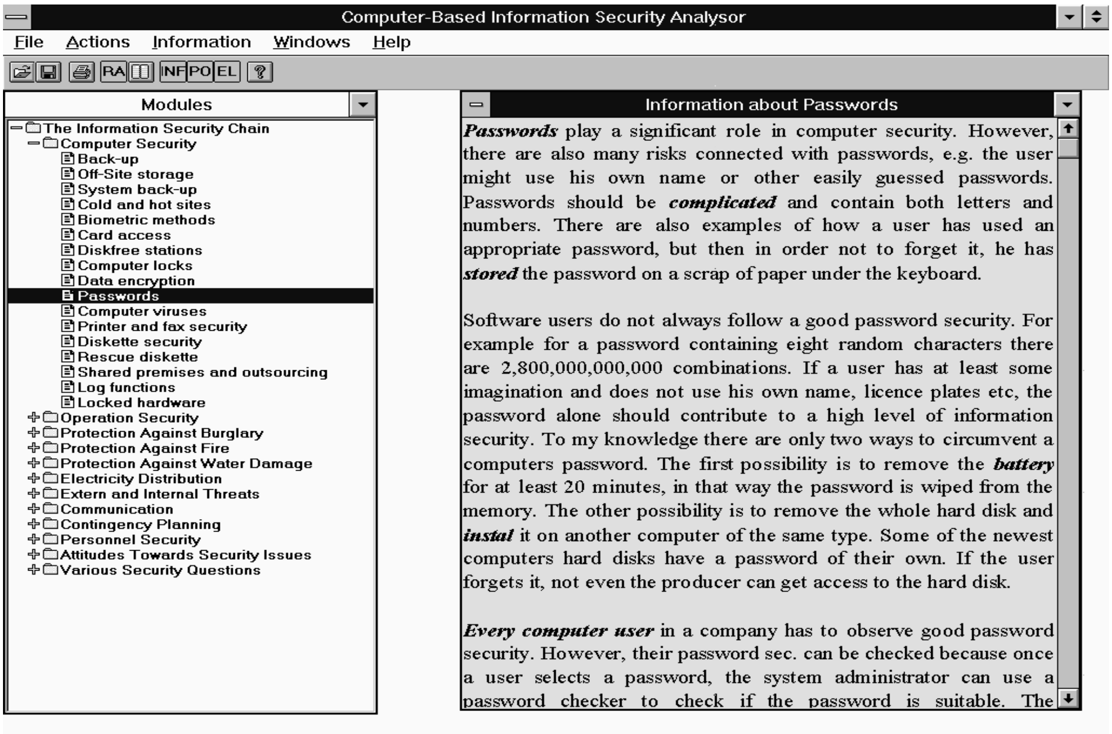

Figure.5: Passwords

Now we have gained information about the submodule passwords. The information is mostly qualitative but to some extent also quantitative. Now we answer the questions about passwords that are included in the database (the questions were added after having used the CBISA in a company). The answers we write down in 'Notes' (see fig.10).

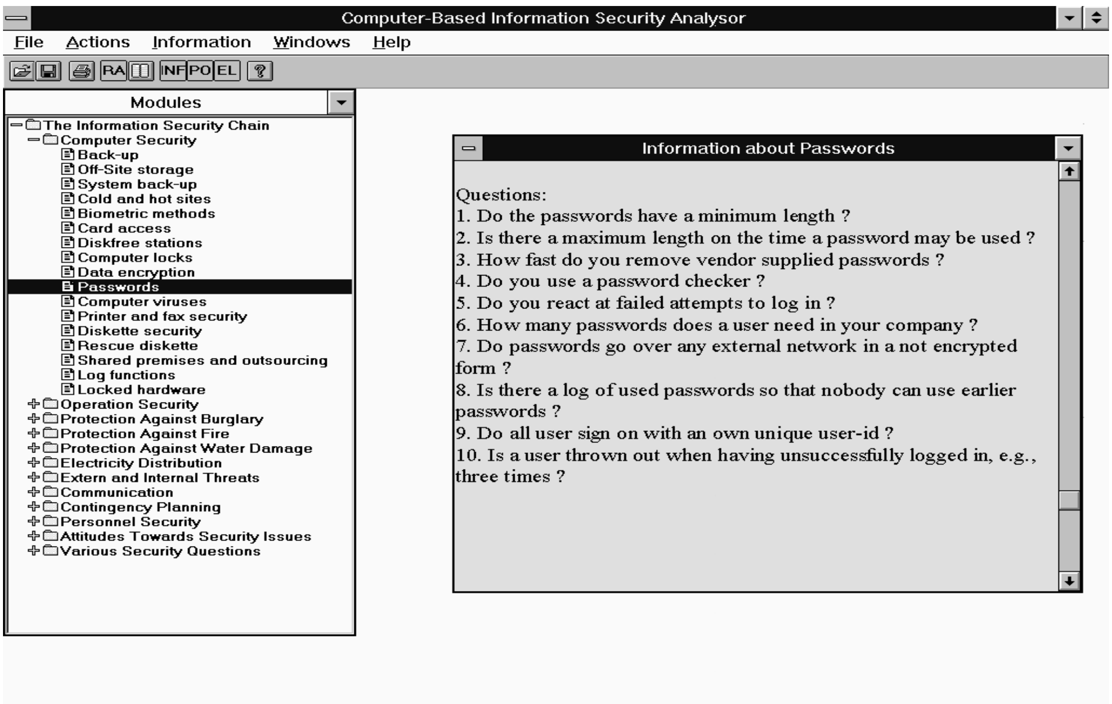

Figure.6. Questions about passwords

As I want to carry out a risk assessment of this submodule, I push the 'RA' button. I select risk assessment because I want to make a quantitative assessment of the company's password security. In the risk assessment I treat those *main resources* that I have in my research found that *ISEC has a major impact on*. In Fig.7. I have put in a few expected losses (after having used the CBISA in a company I improved the RA, see chapter 3.2.).

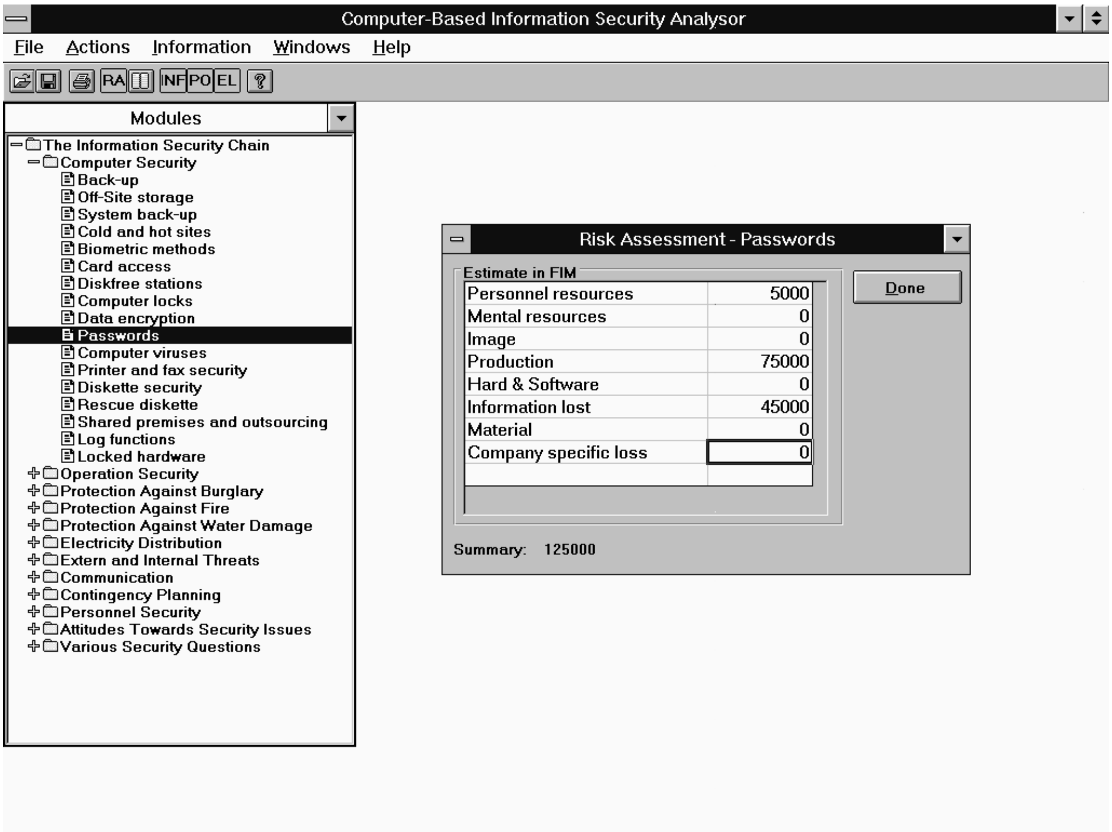

Figure.7: Risk Assessment - Passwords

As I have pointed out the ISPA (Information Security Portfolio Approach) is built into the CBISA. When we have carried out the analysis we can select from the *scroll bar* those 5, 10, 15, 20, 25 or 30 submodules that have brought the *biggest expected economic losses*. The calculated sum we can use as a basis when deciding if the ISEC-improving measures that are to be implemented will be profitable or not. The inbuilt clarifying figure of the approach gives the user an insight into the *ISPA*. Let us say, to make it easy, that, after having performed the whole analysis, we select the 5 submodules with the highest losses. The 'screen' looks like the following:

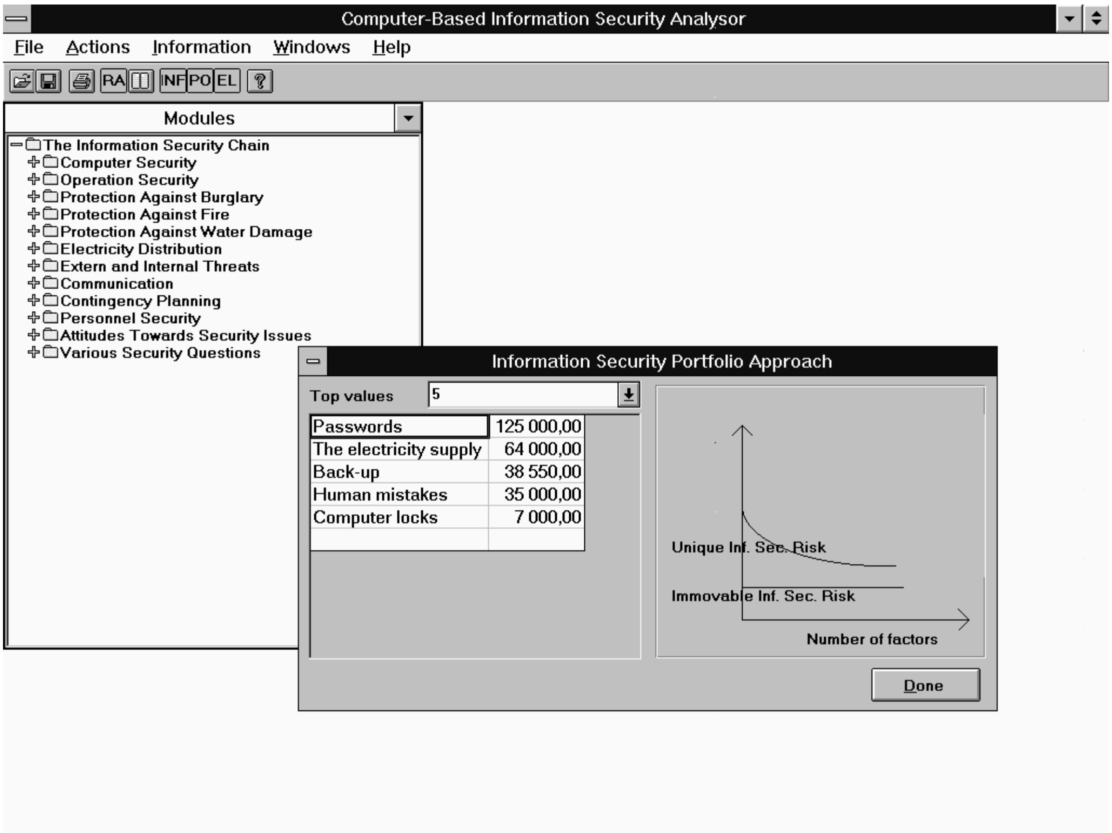

Figure.8: The Information Security Portfolio Approach

The *economic loss table* from the Finnish investigation[10] is included in the CBISA. The data give us the possibility of seeing where the losses have occurred. The user can get access to the data by selecting the *'economic losses' (EL)* button. These data can be used as additional information.

[10] A total of 3309 incidents in ISEC (companies and public organisations summarised) were reported to have occurred during the last five years. When we further asked from where the economic losses specifically came, we got only 172 answers.

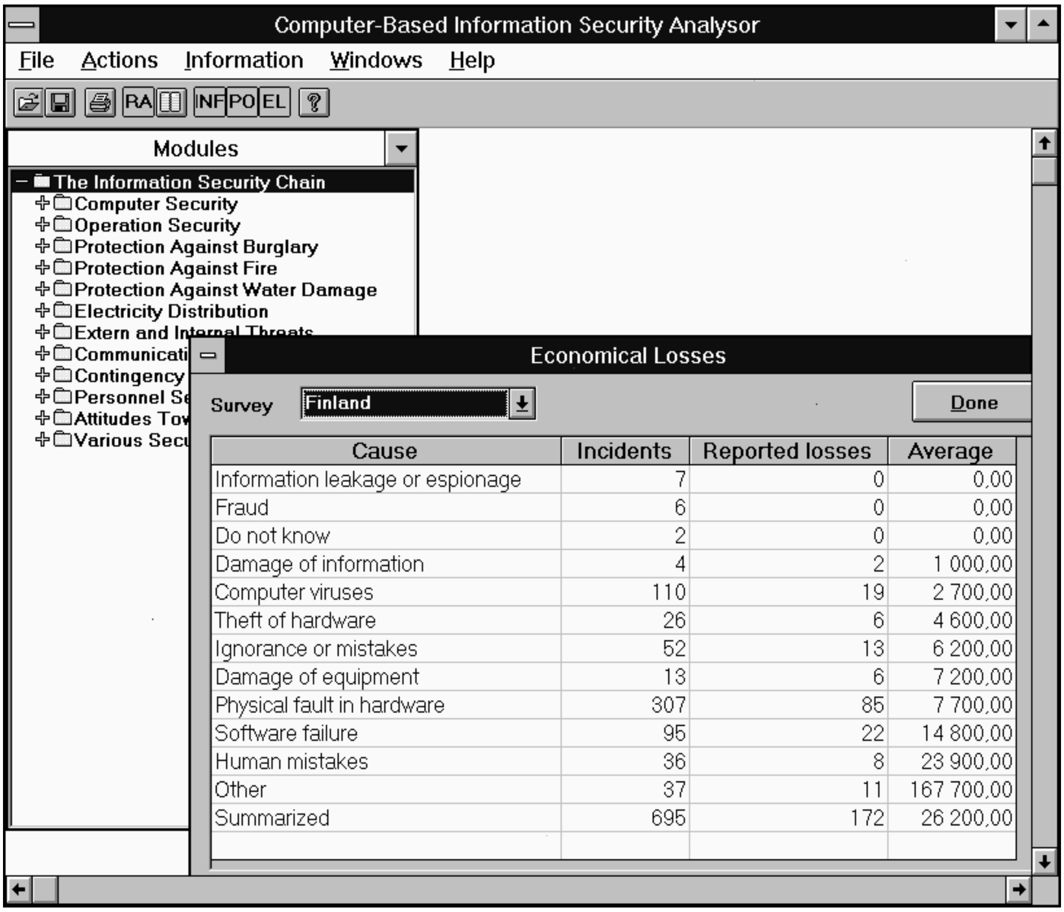

Figure.9: Economic losses

There is also a *help* function that helps the user if necessary. The *help function* contains the most crucial data about how the CBISA works. It is also possible to *make notes* during the analysis. The notes can be made for *every submodule*. Thus we can make decisions during the analysis and write them down. The answers at the questions we can also write down in ‘notes’. 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 (see next page).

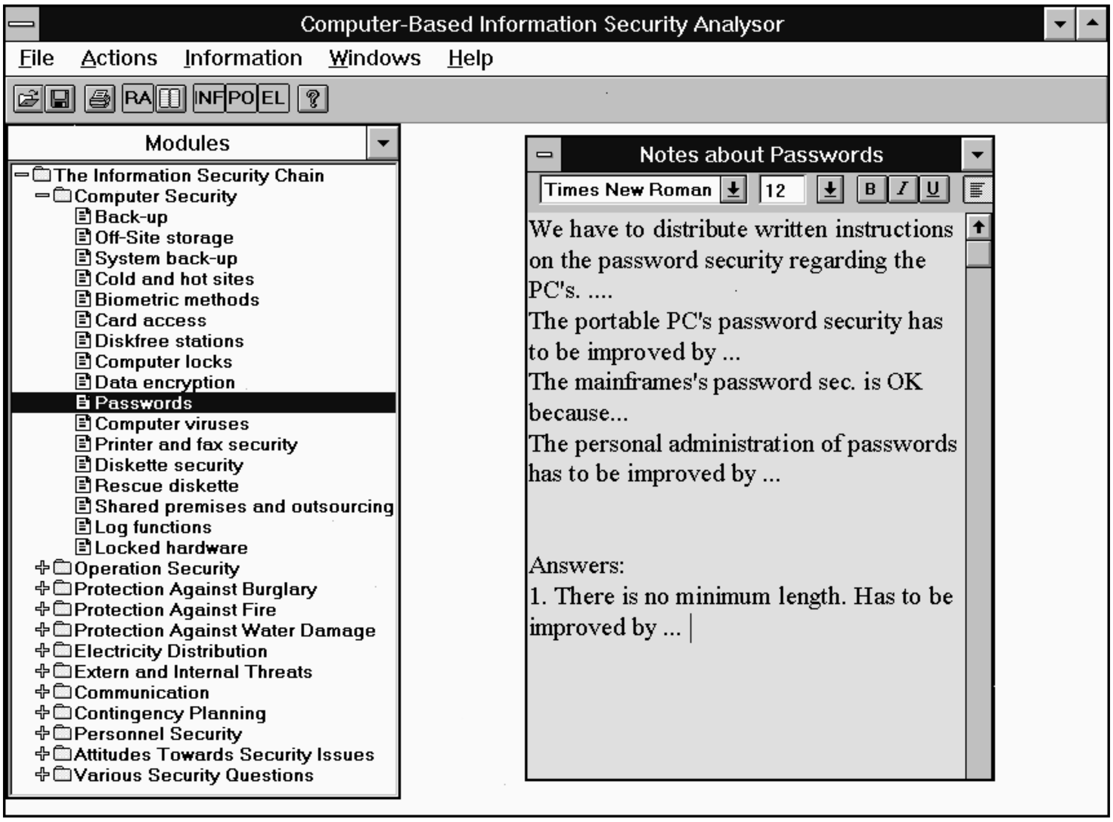

Figure.10: Making notes

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 should also be noted that the CBISA can also be used as a support tool when making a pilot study of the ISEC in a company or to analyse the ISEC without calculating the investment and risks. As I have pointed out the CBISA functions also as a *manual* on information security. Our investigation[11] showed that companies would need a manual on ISEC. In the next chapter I will deal with what the CBISA was like to use in a company and what strengths and weaknesses was found out.

3. USING THE CBISA

In the *project group* we were *6* persons. The company's manager, a representative from central administration, the EDP manager and two of the EDP manager's assistants. The company's manager was not present throughout the analysis but attended altogether a little under one day. Together the company representatives represented enormous

[11] Salonaho, Mikael et al. Suomen tietoturvallisuutta käsittelevän kyselytutkimuksen tulokset, 1994

knowledge in the unit. For three days the CBISA was very thoroughly tested, we found out both its *strengths and its weaknesses.* The analysis I carried out using a *portable computer* connected to an *overhead projector and screen*. By using an overhead projector, each member of the group could follow the stages in the CBISA.

3.1. Benefits of the CBISA

As I navigated in the CBISA for 3 days I found that the CBISA was nice to work with. The *windows* I could easily move and so have many functions in the CBISA running *simultaneously*. When the discussion was intensive and concerned more than one module, I could quite easily *'jump'* between the modules to make notes and risk assessments. Following *good back-up security* I regularly took back-ups on the information.

The *structure* of the CBISA was appreciated by the project group. It was pointed out that by *systematically* dividing the subject into the modules the subject had been made *treatable*. The *user-interface* of the CBISA was considered to be good. This is also a very important fact because if the user-interface is not good enough, working efficiency will suffer. The project group was of the opinion that it was *much better* to have the system *computer-based* than 'paper-based'. It was considered that making the analysis on paper would have been much more *time-consuming*. The notes I made were shown on the *screen* and were sometimes *corrected and changed* by the group. In that way the whole project group could follow up what was written down during the analysis. Without doubt I can say that the CBISA functioned as a *support for decision-making*. It seems to be as Klein et al. considers, i.e., a DSS can improve the communication and collaboration between decision-makers.[12]

The *database* was considered to be large. The project group considered that they had *learned* a lot about information security by reading the information in the database. It was much appreciated that the CBISA was more than "just" computers.

Sometimes we used the *economic losses table*. It was useful as additional information in the discussion that we had. I consider that this part could be enlarged in the CBISA. Economic losses tables from investigations in different countries would function as nice

[12] Klein, M. & L. Methlie. Knowledge-based Decision Support Systems with Applications in Business. 1995

additional information in a discussion. One problem is, naturally, that such material is scarce. In the literature there is much about the lack of data on what economic losses inadequate information security can bring (cf., Parker,81, Saari,87, Caelli,89, Smith,93, Finne,94).

Within one week of the end of the ISEC analysis I sent to the company a report on the analysis. The report was appreciated by the company. The report was further developed in the company with more company-specific *technical* details. The report was built on the division into modules and submodules. The report contained some selected *'key-information'* from the database and the full *notes* made during the analysis.

3.2. Places for improvements

As one member of the project group pointed out, questions could function as a more direct basis. Actually the questions were already in the text, but for further use in companies I *separated* them from the text; this made the CBISA more user-friendly.

A member of the project group considered that the CBISA should be provided with some kind of *graphics* to show the results of the analysis. This is a good idea and will be a subject for further research. Another subject for further research I consider to be *scenario analysis,* which could be further incorporated into the CBISA. This would be possible by including a *'notes for scenario analysis'*. A project group could here even more freely 'brainstorm' around scenarios. For example, how can a computer virus get into our company ? Such 'brainstorming' was already done very much and the results written down in 'Notes', but we could facilitate it by introducing scenario analysis.

The *risk assessment* method had to be improved. Courtney's risk assessment method that I had used first gave us the *directions* of the losses but was not good enough. The project group suggested that the risk assessment should be made *more flexible* and give the user possibilities to put in himself *where* the losses occur, *how big they are* and *how often they occur*. On many modules we carried out a risk assessment but on some of them the scale for economic losses was not appropriate. I developed the RA by dividing up the losses in resources (see fig.7).

4. CONCLUDING REMARKS

The analysis was carried out in co-operation with persons that knew the company very thoroughly. *This was of great importance*. When carrying out the CBISA it is essential to have good *support from the company*. As was pointed out in the 'Guideline for Automatic Data Processing Risk Analysis' the role of management is crucial.[13] Also Smith[14] points out the importance of *support* from top managment for information security.

The problems in ISEC are *unstructured* and I consider that they are appropriate for solution with the help of a DSS. I have built a *KB-DSS* for information security; I consider that the CBISA is a little more than a prototype. One of the strengths of the CBISA is that it is built on a *combination* of quantitative and qualitative assessments. Supported by the CBISA the decision-maker/s is/are able to make decisions that support better information security. The CBISA can be used as a support tool for *making decisions in a group*. However, there is always a chief decision-maker who has overall responsibility. Can we achieve an adequate level of information security when supported by the CBISA ? I consider that the company whose information security we analysed should be able to achieve an adequate level of ISEC if they carry out the improvements that we suggested in our analysis. The results of an ISEC analysis are of a very sensitive nature and have to be adequately protected.

The CBISA is a computer-based *support* system to tackle the *problem* of information security. The CBISA functions as a *framework* for an ISEC anlaysis. Merely by using the CBISA we *cannot improve* the information security in a company. *Human beings have to carry out the improvements.*

With some interesting results I carried out the CBISA in a *small system* which constituted a part of a big system. The CBISA is a research tool that in my further research I will use in industries in order to critically evaluate its impact on how the companies tackle ISEC issues. The tool should be further developed and of great research interest would be to investigate more closely if the use of computer support in ISEC analysis reduces economic losses.

---

[13] U.S. Department of Commerce/National Bureau of Standards. 1979 August 1

[14] Smith, Martin. Commonsense Computer Security, your practical guide to information security. 1993

REFERENCES

Arbnor, Ingeman & Björn Bjerke. Företagsekonomisk metodlära. Studentlitteratur. Lund. 1977

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

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

Finne, Thomas. Creating the Framework for an Information Security Analysis. Institute for Advanced Management Systems Research. Research Report. Åbo Akademi University. Åbo Akademis tryckeri. Åbo. Finland. 1995

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

Microsoft Corporation. Visual Basic/Windows. Visual Basic Version 3.0

Microsoft Corporation. Access/Windows. Access Version 2.0

Murray, William H. Security should pay: It should not cost: In Information Security The Next Decade. Ed. J. Eloff & S. von Solms. Proceedings of the IFIP TC11 Eleventh International Conference on Information Security. South Africa 9-12.5.95, pp 1-6

Parker, Donn B. Computer Security Management. Reston Publishing Company Inc. Reston. 1981

Saari, Juhani. Tietoturvallisuuden käsikirja. OTAVA. Keuruu. 1988

Salonaho, Mikael, ICL Data Oy, LAN Vision Oy. Project group: Aimo Törn, Keskusrikospoliisi, Suomen Kuntaliitto, Vakuutus Oy Pohjola, Erkki Mustonen, Kari Laine, Timo Laine, Leena Meisalo, Marko Helenius, Thomas Finne, Petri Väänänen, Arto Ahti. Suomen tietoturvallisuutta käsittelevän kyselytutkimuksen tulokset. 1994. (Translated from the Finnish language by T.Finne). Åbo Akademis tryckeri. Åbo. 1994

Smith, Martin. Commonsense Computer Security, your practical guide to information security. McGraw-Hill Book Company. London. 1993

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

Walden, Pirkko. Doctoral Thesis. Expert Systems in Strategic Market Management. Åbo Akademi University. Åbo Academy Press. Åbo. 1992

Wood, Charles C. Effective Information Security Management. Elsevier Advanced Technology. Oxford. UK. 1991

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