WHY SAFEGUARD INFORMATION ?

This research report is a preliminary version of a paper to be published in:
Computer Audit Update. Elsevier Advanced Technology, 1996

Thomas Finne
Åbo Akademi University, Institute for Advanced Management Systems Research.

Turku Centre for Computer Science
TUCS Technical Report No 38
23 August 1996
ISBN 951-650-816-2
ISSN 1239-1891

WHY SAFEGUARD INFORMATION ?

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

Abstract
The security of information is becoming increasingly discussed. In this paper I will show why the subject is of importance and what economic losses inadequate ISEC can bring an organisation.

Key words:
Company, economic losses, information security (ISEC).

1. INTRODUCTION

Internet security, encryption, hackers, espionage, computer viruses are all words that are becoming increasingly well-known. One can say that information security is growing in importance, something that soft and hardware producers have recognised, and which they have started to turn into commercial products and services. Information security is becoming one of the buzz-words of the middle 1990's. Why ? Is the importance of the subject exaggerated or is it really an important function in a company. Is there any proof of the importance of ISEC, or is it just a way for producers of ISEC products, hard & software and sellers of ISEC services to create business ? Can a company be hit by serious difficulties if it has not recognized the importance of ISEC ? Is the security officer exaggerating when he says that the investment in ISEC has to be increased ? Below I will list 12 points to show why ISEC is important; then I will present the results of an investigation on ISEC in Finnish organisations. I will also present tables indicating the ISEC breaches and economic losses that companies have been hit by.

2. 12 COMMON REASON FOR ISEC

1.

Decisions are based on information and in a changing and turbulent world information is becoming more and more valuable. The wrong decision can cost the company its existence.[1] Consequently, information has to be reliable, easy to use and should be easily accessible to those authorised to use it. I think that the question of whether ISEC is adequate is *one of the uncertainties* in the everyday life of a company. I consider that when security risks are kept under control, it will be possible to concentrate more resources on the company's daily business operations.

2.

Companies *invest large amounts of money in soft- and hardware*. These investment plays a crucial role in the company's survival. "The value of today's information technology investments is the risk-adjusted, present cash value of committed future productivity gains for the entire business."[2] Information security is a way to *protect*, the usually very large, investments in information technology. The ESF (European Security Forum) points out that information security in the 1990s is the lifeblood of an organisation. Processed by powerful computers and communications networks, information supports critical business functions, and thus provides a competitive edge.[3] Smith[4] writes that: "..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...". We live in a period when information is becoming increasingly valuable. Information also becomes very quickly out-of-date. For example, a database containing vital data about customers, can soon become out-of-date if not regularly updated. A company has to know what information is *most valuable* and put efforts in *protecting that information.*

3.

The *competition* between companies is growing constantly keener and espionage and sabotage are no longer fiction but real-life problems. With increasing internationalisation our business world encounters partners from other business cultures and may risk suffering from actions that they are not prepared for. Parker pointed out at his presentation that there is an intelligent enemy that specialises in getting information. Because of this information security has to be automated. Within a fraction of a second a breach in information security can happen. Crimes are automated; therefore the protection has also to be automated.[5] For example, when a company draws up its strategic plan for the coming 5 years, what benefit would it not be to know competitors' strategic plans ? Huge of course. Another fact is that research

---

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

[2] Strassmann, Paul A. Information Technology and Organizational Effectiveness. 1994

[3] European Security Forum. Protecting Your Business. 1993

[4] Smith, Martin. Commonsense Computer Security. 1993

[5] Parker, Donn. Presentation of the paper: A New Framework for Information Security to avoid Information Anarchy. 10.5.1995

results can be obtained by espionage much cheaper than by actually performing the research. Internationally it is a well known rule of thumb that research results can be illegally obtained with 1/60 of the investment originally spent to achieve the results. Especially for a company in economic distress this could be very tempting. As Ledell[6] points out the business world is becoming increasingly harder and we have to accept that some competitors might have totally different ethical rules of the game from what we have.

Abuse can be very damaging for a company. In a large study in the UK it was found out that most abuse was detected *by chance*.[7] It should not be so that most abuse is detected by pure chance. We can ask ourselves how much abuse remains undetected. Internal control and audit are *crucial* for detecting abuse.

4.
Traditionally thieves have stolen easily cashable assets, for example cash and shares. If the company does not have insurance the economic losses can be very big. However, most companies are insured against "traditional" factors like fire, burglary and water damage. Today it is increasingly common that computer hardware is stolen, because it is quite easy to sell onward. The hardware that a company loses can be very valuable, but the information that the hard disks might contain can be *irreplaceable*. Very few companies are insured against information security breaches.

5.
Software piracy can also be considered as a part of a company's ISEC. According to an investigation software theft cost the industry $17.3 billion world-wide in 1993.[8] Because of these losses some countries have taken action against the problem. For example, in Great Britain organisations have started to offer rewards of up to £2500 to those who report information that leads to successful legal action for the use of unlicensed business software. Similar programmes for rewarding informants have been successful in Australia, Taiwan, Hong Kong and South Africa.[9] A company has to see to that its software licences are kept up-to-date. I also want to point out that computer viruses and malfunctioning software pose much larger threats in *pirated* software.

---

[6] Ledell, Göran. Dataolyckor - har det verkligen hänt någon gång ?. 1992
[7] Audit Commission. 1994, p 12
[8] Collinson, Helen. Computers & Security. No 4. 1994
[9] Computer Fraud & Security Bulletin. November 1994

6.

It is worth noting that the sections that constitute a company's information security can be *defined as factors in Michael Porter's value chain*. According to Porter a company, if it wants to survive, has to achieve a sustainable competitive advantage (SCA*)*. To achieve it, the company has to develop all parts in the value chain into excellence, or at least have a stronger value chain than its competitors.[10] From a national perspective Porter writes that “A nation’s competitiveness depends on the capacity of its industry to innovate and upgrade.”[11] Information security can be seen as one of the factors that a nation and its industry has to keep up with. As competition between countries becomes more intense, a country in which information security issues are disregarded will easily become a target for organised attacks on vital business interests.

Wood[12] writes that “The role of information security is changing - now it can provide a competitive edge, while in the future it will be an essential part of organisational survival”. Saari[13] points out that information security can be made to a standard like customer service, reliability, punctuality etc. According to Porvari information security is also a part of a company’s *strategic planning*. He considers that information security risks should be included in a company’s strategic planning.[14] According to Valli[15] the manager has the ultimate responsibility for the company’s information security. The company’s manager makes the most important decisions and in that way he has a great responsibility together with the person directly responsible for the company’s ISEC. Internationally the responsibility for information security lies more and more on the shoulders of *managers*. In the USA it has happened that managers that have neglected information security have been prosecuted for putting the company at risk.

7.

The development of automatic data processing has been very fast. Enormous amounts of information can be *rapidly processed* and saved on *easily accessible media*. I consider that the standard of information security has not kept pace with this development. Information that before was saved on a large amount of paper and was physically difficult to steal can today be saved on a single disk which can easily be removed. In today’s world companies have to gather and store a lot of information in

---

[10] Porter, Michael. Competitive Advantage, Creating and Sustaining Superior Performance. 1985

[11] Porter, Michael. Harward Business Review. 1990

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

[13] Saari, Juhani. Tietoturvallisuuden käsikirja. 1991

[14] Porvari, Paavo. JERbitti. 1993

[15] Valli, Matti. Yritysjohtaja vastaa myös turvallisuudesta. 1994

order to *compete*. Without doubt a lot of "unnecessary information" is stored. However, the starting point has to be that we protect information by carrying out improvements in information security, not by diminishing the amount of information. Information that seems to be unnecessary today can be *valuable tomorrow*. Where do we draw the line ?

Technical progress is rapid, which places new demands on information security. As Andersson has pointed out, cheap processing has encouraged a return to the widespread decentralisation of data common before corporate mainframes led to centralisation, and along with it, decentralisation of control.[16] According to Miettinen et al. a human being's ability to control complex systems is limited. Therefore information security breaches are not found even during the construction of the systems. The breaches can remain undetected until someone finds them and uses them for his/her own purposes.[17] Progress in technology is extremely fast and it is difficult for a company to keep up with development, especially if the company has not adequate resources to put into keeping up with technological development. The *computerisation of business* has taken place very fast, and those responsible for the process have often had this responsibility imposed upon them *in addition* to their everyday tasks. As a result there has not been enough time to deal with information security questions. The starting position is that those that want a piece of information from a company have the newest technology and expertise. I am convinced that there is no such thing as 100% security. There is always some kind of risk that has not at all, or not adequately, been taken into consideration. There are also risks that cannot be delimited totally, for example, natural disasters.

8.

There seems to be inadequate interest in information security in both companies and public services. From the table below we can see the results of an investigation from the year 1993. The investigation[18] contained 2000 inquiry forms sent to companies and public services in Finland. The response percentage was 30 per cent. Among other things the investigation examined if there is a person appointed to be responsible for the organisation's information security.

---

[16] Anderson, Alison & Michael Shain. Information Security Handbook. 1991

[17] Miettinen, Juha & Jorma Kajava. Tietoturvan Hallinta Nykyaikaisessa Yrityksessä. 1992

[18] Helenius, Marko et al. Tietokoneviruksia käsittelevän kyselytutkimuksen tulokset. 1994

(Answers in percent. Answer percentage = 30%).

	Companies	Local government	State administration
Unanswered	5	5	4
No	67	67	47
Yes	28	28	49

Table.1: Is there a person appointed responsible for the organisation's ISEC ?
Source: Helenius, M. et al. Tietokoneviruksia käsittelevän kyselytutkimuksen tulokset. 1994, p 27

In another investigation (see chapter 3) carried out in Finland a total of *1,800 inquiry forms* were sent to randomly selected companies and public services. We got a total of *521 answers* from the questionnaire, which means an answering percentage of approximately 30. In our questionnaire we asked a similar question to the one above and got the following distribution:

(Answers in numbers. Answer percentage = 30%).

	Companies	Local & State
Unanswered	5	1
No	271	210
Yes	22	12

Table.2: Is there a person appointed responsible for the organisation's ISEC ?
Source: Salonaho, M. et al. Suomen tietoturvallisuutta käsittelevän kyselytutkimuksen tulokset. 1994, p 12

The result of our investigation showed that the situation had got even worse; this is very alarming. Pesonen[19] investigated the security in Finnish companies by sending out questionnaires to 453 companies with over 70 employees. The investigation showed that those made responsible for information security in the companies spent 14.5% of their working time on information security. In an investigation performed in the UK over 80% of the respondents claimed to have a department or individual responsible for information technology (IT) security. However, it is much a question of definition and therefore the true proportion of organisations with a specialist security function may be as low as 15%.[20]

---

[19] Pesonen, Markku. Yrityksen turvallisuusjärjestelyt. 1993
[20] NCC et al. 1994

According to Wright the excuses companies use for minimising ISEC are many. To name a few: security controls cost money, security is difficult to cost-justify, it is difficult to assess the value of information, the security threats are too complex to eliminate and the users do not want to be bothered with security, etc.[21] There are many excuses but it is a fact that inadequate information security can even bring a company to bankruptcy. Wood[22] writes that "The perpetuated biases against information security, the woefully inadequate security models, the reactive and incremental improvement approaches used to address security, the information security infoglut, and insufficient staffing/resources are all symptoms of a most serious problem". According to Wood some managers believe that they should determine how much they should invest in information security by examining what *other companies invest.* However, every company should ask itself how valuable, sensitive or critical this information is for us.[23] In a German survey with 240 participants, it came out that only one of four had carried out a risk analysis on their information security.[24] In the same investigation it was noted that "Die grössten Probleme bei der weiteren Verbesserung liegen im fehlenden Bewusstsein und dem fehlenden Geld."[25]

In 1994 Tallberg[26] sent out a *questionnaire* concerning EDP audit and information security. The participators were the 568 biggest companies in terms of turnover in Finland. He got 116 answers, of which 100 were usable. It was found out that ten per cent of higher management thought that ISEC is of small importance. Sixteen per cent thought that information security is in principle a good thing. Of top management 33 per cent were of the opinion that information security is an important function; 18 per cent thought that ISEC is of strategical importance and 23 per cent did not answer the question. In any case it is worrying that such a large part of top management thought that ISEC is of small importance. Smith[27] points out the importance of *support* from top managment for information security. Both *computer and security personnel* should together work to gain this support and improve information security.

9.

As I have pointed out the trend in computers has recently been moving to *distributed systems*. This means moving from traditional large computers to open client-server

---

[21] Wright, Marie A. Computer Fraud & Security Bulletin. March 1995
[22] Wood Charles C. Effective Information Security Management. 1991
[23] Wood, Charles C. Effective Information Security Management. 1991
[24] KES Sicherheits-Studie. 1994
[25] KES Sicherheits-Studie. 1994
[26] Tallberg, Anders. ATK-tarkastuksen ja tietoturvallisuuden kartoitus; alustava yhteenveto tuloksista. 1994
[27] Smith, Martin. Commonsense Computer Security, your practical guide to information security. 1993

systems. The companies have mostly searched for savings in costs, increased flexibility and the possibility to choose.[28] Andersson[29] points out that there are opinions that this shift to client-server systems will force information security systems to be decentralised. KES Sicherheits-Studie[30] pointed out that information security should be built in at the beginning of downsizing. I would say that information security is a part of the fine-tuning of technology.

Distributed systems, outsourcing, and *time-sharing* have become well-known during the last few years. These quite new things in EDP bring new information security aspects. Time-sharing means that companies share computing services and in that way decrease costs. However, the *information security chain*[31] becomes larger and the information security risks increase. For example, if one of the employees in one of the companies is unreliable, all the companies taking part in the time-sharing can get damaged, instead of perhaps 'just' one company. It is quite common that companies outsource their information system; this may be economically justified but raises some urgent questions about the company's ISEC.

Another new thing in the computer world is the rapidly growing popularity of the *Internet*. The Internet brings new information security aspects. At IFIP TC11 Eleventh International Conference on Information Security, South Africa 9-12.5. 1995, Cohen was of the opinion that there are one billion attacks yearly on the computers connected to the Internet. He also said that the security of 40 per cent of the computers connected to the Internet is breakable.[32] The increasing use of networks and telecommunications has also brought new ISEC problems. As Wong points out, fraud is getting technically more sophisticated. Criminals and hackers have the time and money to refine their techniques.[33] (Auth. rem.: See also the very interesting book: Frontiers of Electronic Commerce, written by R.Kalakota & A.Whinston. 1996. The book deals, among other things, with security issues in electronic commerce).

Mobile computing has become more and more popular. Portable computers and mobile telephones are used more and more frequently. However, the security around them is

---

[28] FISUGbytes. No 3. 1994
[29] Andersson, Ross J. Communications. 1994
[30] KES Sicherheits-Studie. 1994
[31] The Information Security Chain (ISC) consists of all those factors having an impact on ISEC. The factors can be seen as links in the ISC.
[32] Cohen, Frederick. Viruses, Corruption, Denial, Disruption and Information Assurance. 1995
[33] Wong, Ken. Computer Fraud & Security Bulletin. February 1995

not always the best. Cullinane[34] points out that the most common threats to portable information are theft, malicious code and eavesdropping.

10.

The *personnel* in a company has great responsibility for the company's information security. It is of the utmost importance that all employees, and especially those dealing with information, follow strict information security. According to Wood[35] "the person charged with designing, implementing, and/or operating a control should not be the same person who is to be the subject of the control". Parker is of the opinion that good information security has to be awarded, i.e., if employees carry out ISEC they could for example, get some kind of gift.[36] Rewarding employees for good ISEC is a very interesting idea and appropriately carried out it should improve the ISEC.

In 1993 Deloitte & Touche conducted a survey about information protection among top business managers of the Fortune 1000 companies and their equivalents. They wanted to know whether protecting information and information processes was more of a management issue in 1993 than in 1985. The response was a strong and pronounced "yes". Two reasons were given:

- the dramatic increase in the number of people involved in information processing
- the volatility of technology.[37]

11.

According to Pesonen *society* has expectations of a company. It is in society's interest that the company creates jobs for citizens and participates in maintaining economic welfare. Society also expects the company to follow laws and regulations. In exchange society, inter alia, provides the company with basic security (fire, rescue and public safety). The company wants to be as successful as possible. The success of the company can usually be seen from how profitable it is, if the company has a good image, etc. A company strives to reduce the amount of money invested in security and uses the security services that society provides.[38] Thus information security is also a part of a *society's welfare*. Adequate information security guarantees that the company will not be hit by "unnecessary" economic losses because of an inadequate information security. I consider that such losses could directly lead to loss of jobs.

---

[34] Cullinane, Dave. Information Systems Security. Spring 1996

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

[36] Parker, Donn B. Information Systems Security. Winter 1995

[37] Deloitte Touche Tohmatsu. Business Continuity Planning. 1995

[38] Pesonen, Markku. Yrityksen turvallisuusjärjestelyt. 1993

As Morgan points out, the ability to cope with *uncertainty* is a source of power. The ability to deal with the uncertainties in the day-to-day operations of a company gives an individual, group, or subunit considerable power in the organisation as a whole. It can be that those who see power deriving from their capacity to deal with uncertainty try to preserve their power by ensuring that the uncertainties continue.[39] From a national and international perspective this reasoning can also be followed.

12.

As Miettinen points out information security is also a question of *image*. If it is known that a company has problems with its information security, it is a fact that the company will not be looked upon as reliable.[40] According to Pesonen a human being has a *need for security*. For a company this can be seen as:

- customers try to avoid dealing with companies that they see as unreliable and where they do not feel secure.
- employees will not work in a company where the workplace is insecure or the journey to work is insecure.
- if the company's security is not under control the employees' energy will be wasted in worrying about their security.[41]

3. EXAMINING INFORMATION SECURITY IN COMPANIES BY USING QUESTIONNAIRES

Above I have enumerated many things pointing out the importance of information security. However, the most crucial question is whether a company can *save money by investing in ISEC*. Profitability lies in the *avoidance of economic losses* that inadequate information security can bring a company. Losses of that kind are undoubtedly significant. However, it is problematic to assess the economic losses connected to ISEC. Anderson et al. has pointed out the problem of assessing economic losses connected to security; "how to evaluate an asset that has no tangible value: how to place a monetary value on threats that may never have occurred in a particular organisation, or even in similar organisations; and how to choose, from among protection features that interact with each other in unknown ways, a set that is not only cost-effective but also conforms to legal requirements."[42] In the literature on information security there is much about the lack of data on what *economic losses*

[39] Morgan, Gareth. Images of organization. 1986

[40] Miettinen, Juha & Jorma Kajava. Tietoturvan Hallinta Nykyaikaisessa Yrityksessä. 1992

[41] Pesonen, Markku. Yrityksen turvallisuusjärjestelyt. 1993

[42] Anderson, Alison & Michael Shain, Information security handbook. 1991

inadequate information security can bring (cf., Parker,81, Saari,87, Caelli,89, Smith,93, Finne,94). Actuarial data are scart; however, there are some tables that show the economic losses that breaches in ISEC bring. In this chapter I will shortly deal with results of an investigation carried out in Finland during summer 1994. When dealing with investigations of this kind and in this specific area, we have to remember that the real number of losses is probably much bigger than that given by the investigations. Many breaches happen *without anyone noticing them* in a company. Many breaches are just *'forgotten'* and it is a well-known (and understandable) fact that companies do not want to get any publicity about their ISEC, especially not about breaches in their information security. There are also the "usual" problems with questionnaires, e.g. how carefully has the respondent filled in the answers ?

3.1. How we examined the information security in Finnish companies

To gather data straight from the companies we made a *survey using a questionnaire.*[43] The questionnaire consisted of many varying questions that had to do with ISEC. In the covering letter we pointed out that the results would be used for research purposes (results to be published). A total of *1,800 inquiry forms* were sent to randomly selected companies and public services. We set up the following limits on the number of employees for the companies and public services participating in the investigation. A company had to have over *50* employees and public services over *20* employees. We reasoned that in this way we could limit ourselves to companies and public services with considerable information assets. The limitation meant the 1800 organisations were taken out of a commercial database containing approximately *15,000 organisations*. We got a total of *521 answers* from the questionnaire, which means an answering percentage of approximately *30*. From *companies we received 298* answers and from *public services 223*.

We asked in our questionnaire about information on the respondents. We wanted to be able to locate in what branch of business the respondent was. We followed the division of business that the *Stock Exchange in Finland* uses. We then added the 3 last ones concerning public services: 1. Banks & Financing, 2. Insurance & Investment, 3. Trade, 4. Metal industry, 5. Forest industry, 6. Mixed industry, 7. Other industry, 8. Other service, 9. State organisation, 10. Local authority, 11. Schools & Universities,

The following sectors were represented:

[43] Salonaho, Mikael. et al. 1994

Trade of business	*Number of answers*
1. Banks & Financing	7
2. Insurance & Investment	12
3. Trade	41
4. Metal industry	59
5. Forest industry	15
6. Mixed industry	10
7. Other industry	73
8. Other service	81
9. State organisation	120
10. Local authority	93
11. Schools & Universities	10

Table 3: Sectors (branches)

We also wanted to know the *size* of the organisations that participated in the questionnaire. This we did by asking about the respondents' *turnover/budget*.

The respondents' turnover/budgets ?
The scale was: (in million Fmk)
0=no answer, 1=less than 50, 2=51-100, 3=101-150, 4=151-300, 5=301-500, 6=Over 500

Scale:	0	1	2	3	4	5	6	Total
No. of companies:	36	121	74	45	80	48	117	521

Table.4: The respondents' turnover

The number of employees in the company ?
0=no answer, 1=less than 60, 2=61-99, 3=100-150, 4=151-250, 5=251-350, 6=over 350

Scale:	0	1	2	3	4	5	6	Total
1. Banks & Financing	0	0	0	1	3	1	2	7
2. Insurance & Investment	1	0	0	1	1	2	7	12
3. Trade	1	1	3	9	7	16	14	41
4. Metal industry	0	0	4	15	14	6	20	59
5. Forest industry	0	1	0	2	2	1	9	15
6. Mixed industry	0	0	1	0	1	3	5	10
7. Other industry	1	0	6	13	15	14	24	73
8. Other service	3	6	3	25	16	5	23	81
Total	6	8	17	66	59	38	104	298

Table.5: The number of employees in the company

3.2. ISEC incidents and economic losses

A *total of 3 309 incidents* in ISEC (companies and public organisations summarised) were reported to have occurred during the last five years. The incidents were distributed in the following way: (Σ=summarized, ans.=answer, inc.=incident, aver.=average)

Branch of business	No answer	Σans.	No inc.	Σof inc.	Inc. on aver.
1. Local authority	19	74	9	793	10.7
2. Schools & Universities	0	10	1	307	30.7
3. State organisation	22	98	25	403	4.1
4. Banks & Financing	3	4	1	31	7.8
5. Insurance & Investment	3	9	4	255	28.3
6. Trade	5	36	7	367	10.2
7. Metal industry	5	54	10	298	5.5
8. Forest industry	0	15	1	288	19.2
9. Mixed industry	2	8	1	47	5.9
10. Other industry	13	60	5	254	4.2
11. Other service	15	66	7	266	4.0
Public:	41	182	35	1503	15.2
Companies:	46	252	36	1806	7.2
All together:	87	434	71	3309	7.6

Table.6: Reported ISEC incidents

When we asked specifically how the ISEC incidents occurred we got 695 answers:
What caused the ISEC incident ?

	No.	Percentage
Information leakage or espionage	7	1%
Fraud	6	0.9%
Do not know	2	0.3%
Damage of information	4	0.6%
Computer viruses	110	15.8%
Theft of hardware	26	3.7%
Ignorance or mistakes	52	7.5%
Damage to equipment	13	1.9%
Physical fault in hardware	307	44.2%
Software failure	95	13.7%
Human mistakes	36	5.2%

Other	37	5.2%
Total	695	100.0%

Table.7: Causes of ISEC incidents

When we further asked from where the *economic losses* specifically came, we got only 172 answers. The following table shows the number of incidents and reported economic losses in Fmk (£1≈Fmk7)

Cause	No. of incidents	Reported econ. losses	Average
Information leakage or espionage	7	0	no ans.
Fraud	6	0	no ans.
Do not know	2	0	no ans.
Damage of information	4	2	1,000
Computer viruses	110	19	2,700
Theft of hardware	26	6	4,600
Ignorance or mistakes	52	13	6,200
Damage to equipment	13	6	7,200
Physical fault in hardware	307	85	7,700
Software failure	95	22	14,800
Human mistakes	36	8	23,900
Other	37	11	167,700
Total	*695*	*172*	*26,200*

Table.8: Number of incidents and recovery costs

Unfortunately we got only 172 answers on what economic losses the ISEC breaches brought the company. The average economic loss is quite low but if a company is hit by several losses it can experience difficulties. In our investigation only 6 frauds were reported which I consider to be a quite low rate. Are the Finns especially honest or have the frauds not been detected ? There have been a lot of computer virus attacks but on average they have not brought heavy losses. We have to remember that attacks from computer viruses are much more common in schools and universities. The *human being* is the biggest ISEC risk of all. In the tables we can see that human mistakes, fraud etc. have caused heavy losses. Another group that caused heavy losses is *malfunctioning hard- and software*. The category 'other' contains such "traditional" ISEC factors as fire and flooding. Normally these bring heavy losses when they happen.

4. CONCLUDING REMARKS

Every company has, more or less, to cope with limited resources. Therefore a company cannot invest enormous amounts of money to improve the level of information security. It can be quite expensive to achieve adequate ISEC. According to Valli[44], it costs a company approximately Fmk 1000-2000 per employee to achieve and maintain information security. Pesonen came to the conclusion that companies in Finland invest on average Fmk 100 per employee/per year in total security (all security measures).[45] In the USA companies devote to computer security an average of 2-4% of their total investment in information technology.[46] The size of the investment in information security was also something that we asked in our investigation. The question was:
- What amount of resources do you yearly use for *maintaining* your *company's* ISEC[47]:
1. In working years ?
2. In Finnish marks ?

The answers were the following:
1. for 150 companies answering the average was 0.4 working years.
2. for 129 companies answering the average was Fmk 134,000.

If I estimate a working year as Fmk 300,000, I get Fmk 120,000. This sum added to Fmk 134,000 is approx. Fmk 250,000, a lot of money for any company. However, we have to remember that the companies that participated in the investigation were companies with many employees, a large turnover, heavy use of computers (an average of 334 computers) and companies with traditionally high ISEC (banks). With, among others, these facts in mind I claim that companies' investment in information security is inadequate.

It is a fact that it can be very expensive to invest in ISEC, but as Wood points out the information security market has an elastic demand curve. The price of information security goes down when demand grows and more organisations enter the information security market. The consumers of information security products and services think that the costs for ISEC should be low. When costs decrease, demand grows.[48] To be able to direct investment to where it is most needed, it is important to find out those factors (submodules) that are the *most important ones* in the company. In this way a company could direct its investments to those that are most important and in that way improve its ISEC. However, no link in the ISEC chain should be left too weak ! A

---

[44] Valli, Matti. Yritysjohtaja vastaa myös turvallisuudesta. 1994
[45] Pesonen, Markku. Yrityksen turvallisuusjärjestelyt. 1993
[46] Miettinen, Juha & Jorma Kajava. Tietoturvan Hallinta Nykyaikaisessa Yrityksessä. 1992
[47] Salonaho, M. et al. Suomen tietoturvallisuutta käsittelevän kyselytutkimuksen tulokset. 1994
[48] Wood, Charles C. Effective Information Security Management. 1991

particular difficulty is estimating when an information security breach happens. If a company is averse to risk, it will try to protect itself, but a company that is less so will not pay attention to the risk. It is very much a question about the *DM's (decision-maker) approach* to the problem. If the managing director thinks in the *short term*, he will not do anything about the information security risk. It can be that the managing director wants to show economic results and thus avoids investment that he considers "unnecessary" and incurs expenditure. A good way is to divide up the *expected economic losses* into personnel resources, mental resources, image, production, hard & software, information lost, material and a company-specific loss. For example, what would the economic losses be if all our back-up were destroyed ?

ISEC is not only a question about computers, software, files, electricity distribution, documents, etc., but very much a question about the information a human being possesses. The same information that is saved on hard disks under high information security is also "saved" in the *human brain*. I consider that the *human brain is the biggest ISEC risk of all.*

In most companies there should be an ISEC officer. That person should be given a position in the company that provides him with the possibility of taking measures to improve information security. The officer has to have enough *support* from colleagues and be given the possibility to update his/her knowledge in ISEC. Technical development is also very rapid in information security. Every person in an organisation has to become more aware of security questions. I want also to point out that when analysing ISEC, the support from management is of great importance.[49]

The amount of soft & hardware is increasing and the use of electronic connections, e.g., Internet, is becoming more common. For most companies electronic contact with the outer world, for example banks and customers, is necessary. ISEC is an international issue. *There are many facts speaking for ISEC; if a company wants to survive in the future, it has to take ISEC into consideration.*

---

[49] 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

Finne, Thomas. Computer Support for Information Security Analysis in a Small Business Environment. 1996

REFERENCES

Anderson, Alison & Michael Shain. Risk Management: In Caelli, William., Longley, D. & Shain, M. Information Security Handbook. Stockton Press. New York. 1991, pp 75-124

Andersson, Ross J. Communications. Why Cryptosystems fail. Number 11. Volume 37. 1994, pp 32-40

Audit Commission. Opportunity Makes the Thief. Press on Printers. London. 1994

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

Cohen, Frederick. Viruses, Corruption, Denial, Disruption and Information Assurance: 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. 1995, pp 454-468

Collinson, Helen. Computers & Security. Abstracts of Recent Articles and Literature. Volume 13. Number 4. UK. 1994, pp 306-311

Computer Fraud & Security Bulletin. BSA offers rewards to informers. UK. November 1994, p 2

Cullinane, Dave. Information Systems Security. Protection of Mobile Computing Assets. Volume 5. Number 1. USA. 1996, pp 65-69

Deloitte Touche Tohmatsu International. Business Continuity Planning. Republic of South Africa. 1995

European Security Forum. Protecting Your Business. London. 1993

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. 1995

Finne, Thomas. Computer Support for Information Security Analysis in a Small Business Environment. In Small System Security. Proceedings of the IFIP TC11:WG11.2. Ed. Jan Eloff. 1996, pp 73-88

FISUGbytes. Finnish Sun user group. No.3. 1994

Helenius, Marko., ICL Data Oy, LAN Vision Oy, P. Järvinen, E. Mustonen, K. Laine, K. Korvola, T. Laine, H. Lunnas, A. Ahti. Tietokoneviruksia käsittelevän kyselytutkimuksen tulokset. Tampereen Yliopisto. Tampere. January 1994

Kalakota, Ravi & Andrew Whinston. Frontiers of Electronic Commerce. Addison-Wesley Publishing Company, Inc. USA, 1996

KES Sicherheits-Studie. So sehen DV-Betreiber ihre Sicherheit. Deutschland. 1994

Ledell, Göran. Dataolyckor - har det verkligen hänt någon gång ? Studentlitteratur. Lund. 1992

Miettinen, Juha E. & Jorma Kajava. Tietoturvan Hallinta Nykyaikaisessa Yrityksessä. University of Oulu. Department of information processing science. Oulu. 1992

Morgan, Gareth. Images of organization. SAGE Publications. USA. 1986

NCC, DTI, ICL. IT Security Breaches Survey Summary. UK. 1994

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

Parker, Donn B. Presentation of the paper: A new Framework for Information Security to avoid Information Anarchy, 10.5.1995: 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 135-144

Parker, Donn B. Information Systems Security. Security Accountability in Job Performance. Volume 3. Number 4. Winter 1995, pp 16-20

Pesonen, Markku. Doctoral Thesis. Yrityksen Turvallisuusjärjestelyt. Yliopisto-paino. Helsinki. 1993

Porter, Michael E. Competitive Advantage, Creating and Sustaining Superior Performance. The Free Press. New York. 1985

Porter, Michael E. The Competitive Advantage of Nations. Harward Business Review. March-April 1990, pp 73-92

Porvari, Paavo. JERbitti. Tietoturvallisuutta kehitetään voimakkaasti Euroopassa, 1993

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

Salonaho, Mikael., ICL Data Oy, LAN Vision Oy. Supervisor: Aimo Törn. Project group: 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

Strassmann, Paul A. Information Technology and Organizational Effectiveness. Hawaii International Conference on Systems Sciences. Maui. 6 Januari 1994, p 23

Tallberg, Anders. ATK-tarkastuksen ja tietoturvallisuuden kartoitus; alustava yhteenveto tuloksista. Svenska Handelshögskolan. Helsingfors. 21.5.1994

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

Valli, Matti. Yritysjohtaja vastaa myös turvallisuudesta. Tekniikka & Talous. 26.8 1993, p 24

Wong, Ken. Computer Fraud & Security Bulletin. Fighting Mobile Phone Fraud. February 1995, pp 10-14

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

Wright, Marie A. Computer Fraud & Security Bulletin. Protecting Information from Internet Threats. March 1995, pp 6-10

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