FFI-rapport 2007/02558

Evaluating applied information security measures. An analysis of the data from the Norwegian Computer Crime Survey 2006

Janne Merete Hagen

Norwegian Defence Research Establishment (FFI)

26.11 2007

FFI-rapport 2007/02558

1014

ISBN 978-82-464-1282-5

Keywords

Kritisk infrastruktur

Effektivitet

Informasjonssikkerhet

Datasikkerhet

Spørreundersøkelse

Approved by

Håvard Fridheim	Project manager
Jan Erik Torp	Director of Research
Jan Erik Torp	Director

Sammendrag

Forfatteren deltok i arbeidet med Mørketallsundersøkelsen sammen med Datakrimutvalget i Næringslivets sikkerhetsråd (NSR) fra januar 2006 frem til arbeidet ble presentert på Sikkerhetskonferansen i september 2006. Etter dette har forfatteren jobbet videre med analyse av datamaterialet. Rapporten gir en oversikt over dette arbeidet og presenterer resultatet av analysen.

Hvor sårbare er norske virksomheter for bortfall av Internettbaserte tjenester og hvor alvorlige er konsekvensene av de rapporterte hendelsene? Analysen bekrefter at norske bedrifter er sterkt avhengig av IT og Internett, men de som har erfart datakriminalitet, rapporterer at konsekvensene er små. Dette samsvarer med lave anmeldelsestall og lave rapporterte økonomiske tap.

Hvilke sikkerhetstiltak har norske bedrifter implementert for å imøtegå datakriminalitet og hvordan samsvarer praksisen med gode sikkerhetsprinsipper? En taksonomi basert på gode sikkerhetsprinsipper (forsvar i dybden og forsvar i bredden) er utviklet for å besvare dette spørsmålet. Studien adresserer mange sikkerhetstiltak, og to viktige tendenser bør kommenteres: Bruken av forebyggende tiltak synes mer utbredt enn bruken av tiltak som har til formål å beskytte bak ”forsvarsmuren” og redusere konsekvenser av hendelser. Vi ser samme tendens i forbindelse med outsourcing av IT-kontrakter der økonomisk ansvar og erstatning i liten grad er inkludert i kontraktene. Funnene samsvarer også med at en liten andel av bedriftene har rutiner for faktisk å beregne tapene. Dessuten, noen organisatoriske tiltak er undersøkt, og disse synes å være brukt i mye mindre utstrekning enn tekniske modne sikkerhetsteknologier. Det er ingen forskjell på bedriftsstørrelse her, selv om store bedrifter jevnt over har flere sikkerhetstiltak implementert. Sammenholdt med prinsipper for god sikkerhet, er dette en klar svakhet i norske bedrifter.

Rapporterer bedrifter som har implementert sikkerhetstiltak færre hendelser, lavere økonomisk tap og høyere økonomisk avkastning på kapitalen enn dem som ikke har implementert sikkerhetstiltak? Statistisk korrelasjonsanalyse viser at de som har mange tiltak implementert oftere rapporterer hendelser. Vår tolkning er at disse bedriftene er mer sikkerhetsbevisst og har dermed bedre deteksjonsevne. Korrelasjonsanalyser av datamaterialet viser også en signifikant, men meget svak korrelasjon mellom økonomisk avkastning og sikkerhetstiltak. En mulig forklaring ligger at økonomisk resultat avhenger mer av andre variabler enn sikkerhet. Sikkerhet er en bi-innsatsfaktor. Korrelasjonsanalyser av sikkerhetstiltak og rapporterte økonomiske tap viser ingen signifikante sammenhenger, men validiteten på rapporterte tap er lav.

Hva er styrken og svakheten ved undersøkelsen? Den norske Mørketallsundersøkelsen gir verdifull informasjon til både myndigheter og bedrifter fordi det ikke blir innhentet systematisk statistikk på dette feltet. Den kan styrke sin posisjon ved flere tiltak som for eksempel vektlegge tidsseriestudier, høyere kvalitet på spørsmål og mer samarbeid med forskning. På sikt kan den ha et potensial som et informasjonssikkerhetsbarometer som sier noe om trender og nivå.

English summary

The author was engaged in the work with the Norwegian Computer Crime Survey from January 2006 and participated in the work with the design of the survey and the subsequent data analysis. The report gives a brief overview of the work.

How vulnerable are Norwegian enterprises for outages in Internet services and how serious are the consequences of the reported computer crime incidents? The analysis confirms that Norwegian enterprises strongly depend on IT and Internet, but when they experience computer crime the respondents report the real consequences to be small or hardly notable. This result is in line with the marginal reporting of incidents to the police and the reported low/minor losses.

Which security measures have Norwegian enterprises implemented to mitigate computer crime and how does this practice correspond with good security principles? Taxonomies based on good security principles have been developed to answer this question. The survey addresses many security measures, and it is worth noting two important tendencies: first, the use of mature preventive measures is more widespread compared to measures that intend to detect and react if incidents occur; second, when outsourcing IT operations, liability and sanction are rarely included in outsourcing contracts. These findings can also be connected with the low percentage of enterprises that have routines for calculating the economic losses of computer crime. Moreover, a few organizational measures are examined in the survey. These measures are less used than preventive security technologies. User education and exercises are rarely used. Compared with good security principles the results reveal several holes in enterprises' security strategies, particularly behind the perimeter security.

Do enterprises that have implemented many security measures report fewer incidents and less losses, or higher financial returns compared with those that have invested less in security measures? The answer to the first part of the question is clearly "no". Correlation analysis shows that those that have implemented more security measures more often report some kinds of security incidents in contrast to those that have not implemented measures. Also, the analysis shows a statitically significant, but weak (low absolute value) correlation between security measures and return of investment. One explanation may be that return of investment is rather due to management factors than security. Security is a bi-factor input. Correlation analysis of security measures and economic losses reveals no significant relationships.

What are the strengths and weaknesses of the Norwegian Computer Crime Survey Questionnaire 2006 and process, and how could the survey become a security measurement tool for the government? A SWOT analysis shows that the survey can come to hold a significant position since statistics on computer crime is lacking. This requires, however, an analytical framework and an improvement of the quality of the survey questions.

Contents

Preface

This report is part of my PhD-study “Measuring the effectiveness of information security measures”. I work as a Research Fellow at the Norwegian Defence Research Establishment (FFI) while pursuing my PhD at the University of Oslo /UNIK and at Gjøvik University College. The PhD study is part of the Critical Infrastructure Protection Project (BAS5) at FFI. The aim of the report is to describe the information security practices of Norwegian enterprises and their experiences with computer crime. A second aim is to use the survey data to search for statistical associations between security measures and effectiveness indicators. The report offers an overview of the survey, the data and its limitations, and presents the main findings from my search for statistical associations.
The target group of the report is primarily other scientists with knowledge in statistics and computer science. In order to make the report accessible for a larger audience, summaries are provided at the end of the sub chapters.

I would like to thank Kim Ellertsen, Næringslivets sikkerhetsråd (NSR)[1], for inviting me to join the work with the Norwegian Computer Crime Survey 2006 during the period from January 2006 to September 2006, and for permitting me to use the data for subsequent analysis. I would also like to thank Professor emeritus Pål Spilling, UNIK/UiO for advising and motivating me during the writing of the report, Professor Jan Hovden, NTNU, for assistance regarding statistical analysis, and Principal Scientist Håvard Fridheim and Research Fellow Hanna Rogan, FFI, for language vetting and general comments on structure and readability. Also, I wish to thank Håkon Styri, PT, Ellen Hagelsteen, OD, Cort Dreyer, MOD, Tor Ottersen, SHDir, Truls Teigen, FFI, Ronny Windvik FFI and Camilla Olsen, FFI, for comments to the report draft.

Janne Hagen
Kjeller, 31st October 2007

[1] The Norwegian Security Council

1 Introduction

1.1 Background

Norwegians extensively use financial, commercial and news services on the Internet. In 2007, about 80% of the households have access to the Internet and 85% of these are connected to the Internet by broadband [31]. This is an increase compared to 2005, when 64% of the households had Internet connections, and 75% of them had broadband. Statistics also show that trade on the Internet still increases. In 2005, 55% of the Norwegian population used the Internet for shopping [23], in 2007 the rate had increased to 60%.

The development of computers and the growth of the Internet have changed the way we live and work. Computers amplify our mental power, allowing us to perform complex calculations and to store, retrieve, and manipulate vast amounts of information. They extend our intellectual reach [22]. The Internet gives us unrestricted possibilities to communicate and share information, and large amounts of information can be forwarded easily and at no cost. But also criminals have access to advanced information technology that enables them to share information and more efficiently plan and execute their criminal actions. Their method of operation mirrors the society they live in. Crime is not new, but the environment where crime is performed has changed as more people have been connected to the Internet. A short historical flashback illustrates this. In the former times, the criminals relied on horses to get away. In the industrial age, cars helped them flee from the police. Cars could be stolen, and highways facilitated a quick escape. In the information age, the situation is just the same: The criminals use the available technology (computers) and weapons (hacker tools), utilize the vulnerabilities (in software and people) and perform sequential attacks. The police are not prepared and poorly equipped. Geographical constraints prohibit an effective investigation [21]. The economic and personal consequences of security breaches can be huge. Critical business information, patents and identities can be stolen. Attack on web sites, which are used for promotions, sale, and public relations, can destroy the reputation of a company, and denial of service attacks can shut down the shop or service temporarily. Although external attacks from the Internet sounds terrifying, trusted people inside the enterprises may constitute an even larger threat [33], in particular if they cooperate with external threat actors.

Despite the fact that computers have been an important part of business life since the 1980s, Norway still lacks good statistics on computer crime. There are several reasons for this. Very few computer crime incidents are reported to the Police, and Statistics Norway (SSB) collects no computer crime data on a regular basis. In addition, computer crime is difficult to detect compared to traditional crime. Surveys on the dark figures of computer crime came as a response to this situation [3]. The first computer crime survey was carried out in 1989. This and the subsequent computer crime surveys examined the number of computer crime incidents detected in a sample of Norwegian organizations. An analysis of the deviations between the reported incidents in the surveys and the incidents reported to the police as a criminal offence revealed large dark numbers of computer crime.

The author was in late December 2005 invited to join the meetings of the Computer Crime Committee at Næringslivets sikkerhetsråd (NSR), and thus got the possibility to influence the design of the questionnaire for the Computer Crime Survey 2006, participate in the analysis and use the data for subsequent analysis. The goal of this report is to document the work with the design of the questionnaire, and present the results and a measurement framework for future surveys based on good security principles. The developed framework consists of taxonomies that visualize different aspects of security according to good principles of security. Compared to the traditional way of simply listing the findings, this framework makes it easier to analyze the outcome of the survey and draw conclusions on the security performance of the organizations. In addition, a method for analyzing the relations between security practices and security/financial performance is presented and applied. Finally, a SWOT analysis is performed to discuss the survey process and questionnaire with the goal to enable improved measurements of information security and computer crime in the future.

1.2 Research questions

This report addresses the following questions:

1. How vulnerable are Norwegian Enterprises for outages in Internet services and how serious are the consequences of the reported computer crime incidents?
2. Which security measures have Norwegian enterprises implemented to mitigate computer crime and how do these practices correspond with good security principles?
3. Do enterprises that implement many security measures report fewer incidents, less losses, or higher financial returns than those that do not?
4. What are the strengths and weaknesses of the Norwegian Computer Crime Survey Questionnaire 2006 and process, and how could the survey become a security measurement tool for the government?

2 Related studies

2.1 The history of the Norwegian Computer Crime Surveys

Norwegian Computer Crime Surveys have been carried out in 1989, 1993, 1997, 2001, 2003 and 2006. The purpose of the surveys has been to estimate the numbers of computer crime incidents in Norwegian enterprises and, later, also the use of security technologies. The surveys have provided valuable information on computer security incidents and related consequences, as the statistics from the police do not provide sufficient information on the threats against information systems. They have revealed large dark numbers and a huge gap between the numbers of computer crime incidents that were detected and the corresponding numbers reported to the police.

In 1989, the first computer crime survey collected data on computer crime incidents among 489 Norwegian enterprises. While the surveys prior to 2001 examined computer crime incidents only, later surveys were expanded to include questions regarding the use of security technologies to detect and prevent incidents. The 2001 study [19] also documented for the first time a positive relationship between investments in preventive and detective security technologies and incident reporting. This finding was confirmed in the 2003 survey [3]. In addition, the 2003 survey concluded that many enterprises had not implemented highly necessary security measures and that the dark numbers were probably even higher than reported by the survey. The 2006 survey expanded the questionnaire to also include organizational security measures like for instance plans and procedures, to provide a more holistic measurement on security status. This approach was new compared to previous surveys. In addition, the 2006 survey also emphasized the study of security in critical infrastructures, and did not focus on public and private sectors the way the previous studies did.

Different types of questions and variations in sample structures (combination of industries and sizes of enterprises) make it challenging to compare the results of the 2006 survey with previous studies. The 2006 survey has for instance a much higher number of answers from small enterprises with less than 200 employees (75%) compared to the 2003 survey (52%). As we know that small enterprises have implemented fewer security measures than the big ones, one should be careful when comparing the different surveys in order to identify trends. Findings of the 2006 survey are, however, compared to and commented in relation to findings of the previous survey of 2003 when equal questions are addressed.

2.2 A summary of Computer Crime Surveys in other countries and comparisons with the Norwegian Survey

Table 2.1 Comparison with foreign computer crime surveys shows a summary of several computer crime surveys. While the Swedish survey “Mörkertalsundersökningen 2005” [12] focuses solely on computer crime incident reporting and dark numbers, the other surveys examine security incidents and security practices. The “DTI Information Security Breaches Survey 2006” [10] and the “2006 Australian Computer Crime & Security Survey” [11] examine a number of managerial and organizational security measures and is thus relevant for comparisons regarding organizational measures. The “2005 FBI Computer Crime Survey” [2] focuses on security incidents and use of security technologies. The “2006 CSI/FBI Security Survey” [9] puts emphasis on cost and measurements of information security as well as security technologies, while organizational security measures are only briefly treated.

A comparison between the different surveys reveals that the samples vary with regards to enterprise size. Due to the different composition of samples, it appears difficult to directly compare the survey results in order to illustrate differences between nations. The response rate also varies greatly. The Swedish survey has the highest one, and is the only one with more than 50% response rate. The UK survey does not inform about the response rate.

Table 2.1 Comparison with foreign computer crime surveys

Survey	Response rate % (responses)	Interview method	Enterprises size profile
Mörkertalsundersökningen 2005	68% (500)	Telephone interview	50% of the respondents have 50-199 employees
DTI Information Security Breaches Survey 2006	- (1001)	Telephone interview and meeting with ISF	A combination of ISF and other UK businesses
2006 Australian Computer Crime & Security Survey	19% (389)	Online, web based	37% have less than 500 employees
2005 FBI Computer Crime Survey	9% (2066)	Hardcopy	88% have less than 500 employees
2006 CSI/FBI Security Survey	12% (616)	Hardcopy and email	36% of the respondents have less than 500 employees
The Norwegian Computer Crime and Security Survey 2006	37% (749)	Hardcopy	88% have less than 500 employees

2.3 A short introduction to performance measurement of information security

The literature provides some guidelines concerning information security measurements. The National Institute for Standards and Technology (NIST) defines metrics as “tools designed to facilitate decision making and improve performance and accountability through collection, analysis and reporting of relevant performance-related data” [26][2]. The purpose of the measurement is to monitor the status of the measured activities and facilitate improvements in those activities by applying corrective actions based on the observed measurements.

According to NIST, IT security metrics should provide quantifiable information for comparison purposes, apply formulas for analysis, and track changes. Percentages or averages are most commonly used for measurements, but also absolute numbers are useful in some situations.

One should distinguish indicators from metrics. A metric is recognized by a predefined structure, while an indicator operates on a more general level. Good metrics are recognized by several factors: a defined scope, based on a predefined model of the problem they describe, a well defined measurement process, repeatability, relevance and cost-effectiveness [27]. In [6], the authors provide guidance for establishing a baseline to begin the process of measuring the costs

[2] See page 9.

and benefits and the effectiveness of their asset protection program. By using a fictitious company they illustrate how a security metrics management program can be established and operated.

When comparing the measurement performances presented in this report to the theory of security metrics, it appears that this report's performance measurements do not fulfil the requirement to be categorised as metrics. Thus, the presented performance measurements are better described as security performance indicators.

The NCCS06 applies three types of information security performance measurements; the compliance with best practices, the number of reported incidents and the financial performance for the last year.

If we trust that following best practice provides the best achievable security level, measuring against best practices could provide useful information about the security level of the enterprises. However, we know that even if the right security measures are implemented, there may be weaknesses in their practical implementation that can reduce the effectiveness of the measures [14]. Correct configurations of security technologies and patching and updating routines may impact the quality of the implemented security technology. Similarly, education of employees can be of both good and poor quality.

Performance measurement of information security by measuring the absence of computer crime incidents requires that all incidents are detected. As documented by [19][3], and later illustrated in this report, underreporting of incidents is a problem even in surveys.

A third approach is to measure security practice against some kind of organizational performance, for instance financial performance. The 2006 survey has also registered certain financial information, such as reported losses and financial performance before tax. Hence, it should be possible to examine also these relations. The relations are, however, not necessarily obvious, due to non-security factors that impact the financial performance of the organization and that vary among enterprises. Examples of factor are the effectiveness of the production process and the strength of the industrial competition. Alternatively, one may examine the reported economic losses of computer crime incidents, but as shown later in the report, these estimates (if reported at all) are very rough at best, and the numbers are uncertain because few enterprises have routines for calculating such losses.

Despite these shortcomings, this report exemplifies how the three kinds of measurements – best practices, security incidents and financial performance – can be used to provide some information on security performance.

3 Methods and materials

3.1 Strengths and weaknesses of surveys

Surveys are popular as measurement tools within social sciences. A target group is invited to answer structured questions, and the respondents are expected to answer honestly and to their best knowledge. Anonymity is provided by the analyst to the respondents to encourage honesty and openness. Simple questions are provided to reduce the risk of ambiguity. There is, however, no guarantee that the respondents don't lie or misinterpret the questions, yet they must be trusted. Very unlikely answers, also called outliers, could be excluded in the analysis. This may result in a lower response rate and also the risk of excluding abnormal incidents that still might be true. Despite these shortcomings, surveys are a popular and practical way to collect large amounts of information at an acceptable cost.

Other scientists who have applied surveys to do research on information security [8] have experienced that it is not easy to collect good data on security practices. People are reluctant to share information on security for several reasons [4]. The fear for the enterprise reputation is one reason. Another reason is that IT security officers fear for their jobs, and a third one is that the respondents fear that criminals can use the information or findings from the survey to attack the enterprise later. Comparing several computer crime surveys, low response rates seem normal, although it can be improved by using "the right" data collection techniques. If we compare the response rate of some computer crime surveys [9][10][11][12], we see that telephone interviews give a higher response rate than questionnaires distributed by mail.

Related to information security, another criticism against surveys can be directed to the number of reported computer crime incidents: How do we know that the respondents have detected and reported all attacks? These questions are highly relevant due to the non-transparency of electronic communication among computers connected to the Internet. It is, for instance, possible to distribute sensitive information to unauthorized recipients without leaving visible finger prints. Thus, the management of the attacked enterprise may not know about the attack. Therefore the answer is that we do not know. In fact, we have no evidence of the total number of reported security breaches. At best we have an indicator, which may provide us with some information on security performance.

It could be argued that the controllable experiment is a better way to collect reliable data to evaluate the effectiveness of security measures. On the other side, it would be necessary to do a large number of experiments to collect the same amount of data available from one survey. A well-developed survey could therefore be a good starting point to examine the security practices and the relation between security measures, security incidents and economy.

3.2 The Norwegian Computer Crime Survey 2006, the data collection process and the responses

3.2.1 The Computer Crime Committee and the Survey Process

The Norwegian Computer Crime Survey 2006 was carried out by Næringslivets sikkerhetsråd (NSR) in cooperation with the Norwegian Center for Information Security (NORSIS) and The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM).

The members of the Computer Crime Committee 2006 at NSR were:

- Øyvind Davidsen, IT Security Manager, Statoil, and Executive Leader of the Committee
- Kim Ellertsen, Chief Executive Officer at NSR
- Berit Børset Solstad, Assistant Chief of Police at ØKOKRIM
- Ove Olsen, Project Leader, SIS and SINTEF
- Tore Larsen Orderløkken, Executive Manager, NorSIS
- Christophe Birkeland, Director of Department, NorCERT
- Arne Tjemsland, Senior Consultant at Secode Norge AS
- Jan Gusland, Consultant, Komplett AS

The author of this report was invited to join the meetings from January 2006 and to participate in the design of the survey and the analysis of the data. In addition, Perduco AS assisted with designing the survey, distributing the questionnaire, registering the answers and producing preliminary frequency statistics. The committee met six times, first time 15th December 2005. The first three meetings were dedicated to the design of the questionnaire while the last ones were used to discuss the results. The results were presented at the NSR Security Conference 20th September 2006.

3.2.2 The population and the sample

The population of the survey was all active Norwegian enterprises (public and private) with more than 5 employees. In April 2006 a random stratified sample of 2000 enterprises was drawn from the Norwegian Register of Business Enterprises. The strata contained 400 respondents (20%) with 5-9 employees, 800 (40%) respondents with 10-99 employees and 800 (40%) respondents with more than 100 employees. The 2000 questionnaires were distributed by postal mail. In June, after one reminder, 749 questionnaires were returned, which gave a response rate of 37%.

The answers seemed to fit well the strata profile of the survey. The distribution of the answers is shown in Table 3.1.

Table 3.1 Answers and the number of employees

Number of employees	**Number of received answers**	**Percentage of total answers**
No answer	*9*	1.2
1-5	*38*	5.1
6-10	*117*	15.6
11-24	*149*	19.9
25-199	*249*	33.2
200-499	*96*	12.8
≥ 500	*91*	12.1
Total	*749*	100

Answers from large enterprises (more than 500 employees) were overrepresented (12.1%) in the survey when compared with the population of all Norwegian enterprises. The majority of Norwegian enterprises are small enterprises. Enterprises with 1-5 employees make up 80% of the total population, and the group with 5-10 additionally 7%. The large enterprises with more than 500 employees amount to just 0.5% of the total number of Norwegian enterprises, but employ as much as 45% of the work force[3].

The distribution of the respondents in the survey is shown in Table 3.2. Most questionnaires were answered by IT managers, followed by business managers. Cross tabulating enterprise size and profession of the respondents shows that in the smallest enterprises, answers to the questionnaire were for the most part given by the business managers. In the largest enterprises answers were usually given by IT managers or security managers. In the medium sized enterprises there were no dominant professions among the respondents.

Table 3.2 Distribution of the respondents by profession

Profession	**Number of responses**	**Percentage of total respondents**
No answer	*55*	7.4
Business manager	*263*	35.1
IT Manager	*307*	41.0
Financial Manager	*94*	12.6
Security Manager	*30*	4.0
Total	*749*	100

[3] The numbers were given by Perduco.

Only 5.7% of the 725 responding enterprises in the survey belonged to the public sector. 24 enterprises did not answer the question about which sector they belonged to. Thus the overall majority of the enterprises in the survey are private businesses. The following definition of critical infrastructure enterprise was provided in the questionnaire: *If you are a critical infrastructure enterprise, then a stop in the service or goods deliveries will result in acute and critical consequences for a large part of the society.* 11% of 739 enterprises answered that they defined their business as critical infrastructure. The critical infrastructure enterprises consisted of 44% of public sector enterprises, and they were also dominated by large enterprises.

Of the 732 enterprises that participated in the survey, 2.9% belonged to the primary industries, 8.5% to personal services, 15.2 % to construction, 22.5 to commodity trade, hotel and restaurants, 22.7% business services and 23.6% to industry etc. This matches the structure of Norwegian enterprises, with exception of the primary industries; when micro enterprises are excluded, farmers typically drop out.

Summary: The answers offer a representative picture of Norwegian enterprises.

3.3 Developed taxonomies applied to the Norwegian Computer Crime Survey 2006 (NCCS06) to measure security performance against good security practices

3.3.1 Threats to an enterprise and computer crime incidents investigated in the survey

A threat is a potential incident; thus it has not yet occurred. When an attacker has utilized vulnerabilities, the threat becomes an *incident or a security breach*. There are numerous threats to an enterprise. Not all become incidents. Potential attackers can utilize weaknesses of employees, the organization, the network architecture, software and physical security. The NCCS06 examines real incidents, not threats. Security breaches included in the survey consist of eight incidents that can be defined as computer crime incidents according to the computer crime law. Additionally, two crime incidents that are related to other crime laws were included because the computer crime committee at NSR wanted to examine them. These incidents are thefts of IT equipment and extortion attempts, which are regarded outside the computer crime definition. Thefts of equipment are crimes for profit, although it is linked to computer crime because of the data inside the stolen equipment. Extortion attempts are actually not a computer crime event, although the blackmailer uses IT systems as a tool in the process.

In this section the author first introduce a broad spectrum of information security threats to an enterprise. Then we describe the incidents addressed in the NCCS06. The deviation is then commented on. The purpose is to visualize the broad range of threats and how the incidents in the survey constitute a subset of the spectrum of potential threats. It shows that the computer crime survey covers only a small subset of all potential security breaches.

Employees can *unintentionally* misuse software, web mail, email and import infected information. They can also disclose confidential or sensitive information unintentionally. Disclosure of information can be performed as one action, or in combination with unintentional misuse. Unintentional misuse of IT resources is pointed out to be a significant problem which also reduces the productivity [32] [34]. An IT support employee explained it this way: "*New technology develops rapidly and increases the usability, but increases the risks. Employees are not aware of these new risks. They also mix private and work related use of IT, but they do not intend to harm their employer. This is the main challenge and a daily task that must be handled*".

Employees can also *intentionally* misuse IT resources and disclose information. The motives can be profit or revenge. They can perform sabotage motivated by revenge by modifying sensitive information or leaving software bombs. Employees can also cooperate with external attackers and provide unauthorized access to third parties[4]. An external attacker can, on the other hand, use the inherent weaknesses in human nature and fool employees to perform actions that lead to security breaches, or perform an extortion attempt [35]. Employees can be recruited by criminals or planted in enterprises by criminals. According to the Norwegian Police, a tendency is that international organized crime and crime for profit merge. As much of the corporate values today are saved in computers and in brains, it seems apparent that criminals and attackers will seek towards these sources, e.g. the IT systems and the humans in the organizations. The Symantic Threat report [37], Norcert and the Police confirm that an increasing share of IT related attacks are well motivated, and that the attackers know very well what they are looking for[5].

External attackers outside the enterprises can utilize weaknesses in *network architecture,* and use software to perform automated attacks. Attacks can be both economic and political motivated[6] or just be performed as jokes. The Internet enables criminals to perform crime from locations far away and escape in a nanosecond. Denial of service attack (DoS) is a typical example of an external automated attack that utilizes the connections in the Internet architecture. Such an attack is difficult to prevent. Weaknesses in the enterprise intrusion detection or defense barriers can also be utilized by external attackers to get unauthorized access. According to Bruce Schneier [24], there are three trends that indicate continuous and dangerous attacks in the future:

1. Fast automation makes attack with a minimum rate of return profitable. Attacks that were just too marginal to be noticed in the physical world can quickly become a major threat in the digital world. There are also huge possibilities for data mining and intelligence.
2. Actions performed from a faraway location can be profitable, due to differences in law and regulations in the various countries.

[4] One example is shown here: Mafia snuser på norske vektere. Aftenposten. http://www.aftenposten.no/nyheter/iriks/article1173273.ece Downloaded 05.10.2007.

[5] Målrettede dataangrep og andre trusler på Internett, NSM, and Problemorientert politiarbeid, Politidirektoratet, Speaches provided at NSR Security conference, September 2007.

[6] It is known that Linux supporters have made viruses to attack for instance Microsoft, but the political ambitions reaches also international politics, like the Russian attacks on the Estonia web site, Kreml angriper Estlands datasystemer, TALLINN (VG Nett) http://www.vg.no/pub/vgart.hbs?artid=184703. Downloaded 16.11.07. Viruses could also be written just for fun.

3. Only the first attacker has to be skilled, as others can use his software. Many sites allow you to download computer viruses and malicious code.

Weaknesses or modifications in the intrusion detection systems may increase the risk of not detecting an intrusion or reacting too late. The last years, enterprise internal wireless access has become more common, and although the security has improved, there may still be a significant risk of information leakages from such networks.

Software carries inherent vulnerabilities which can be utilized by external or internal attackers. Software is often launched on the market before it is tested properly, and when security patches are released later on, the decisions to install the patches depend on the subjective judgments of the IT support employees. Also weaknesses in the host system access control, such as weak passwords and non-updated access controls, can be utilized to get unauthorized access. The story of Cliff Stoll [25] exemplifies how a hacker operated and took over the user account of an employee who had left a year ago, and even obtained administrator rights. The spy used the computers belonging to Lawrence Berkley Laboratory in order to acquire defense secrets through Arpanet and Milnet. He left trojans and stole passwords, this way gaining access to several user accounts. He also stole the encrypted password files and decrypted them. The algorithm was known, so by trying different plaintext passwords, he finally found the right ones. Stoll wrote the book after spying on the spy. It is also well known that operating systems and application software have inherent weaknesses; new security patches are frequently distributed by software vendors. These weaknesses can be utilized by attackers in the period between the weakness is detected and a patch is distributed and installed. This “window of opportunity” is increasing. Unintentional or intentional import of infected material such a virus, worms, trojans and root kits typically utilizes weaknesses in software.

Weaknesses in *physical security* should not be overlooked. Servers located in non-protected areas can be rebooted with infected software by disgruntled employees or spies. Similarly, backup systems can fail or be sabotaged. PCs and other kind of IT equipment, which is not physically secured, can also be stolen from offices or homes. Electric power systems that computers depend on can moreover be sabotaged or simply break down. Likewise, fire or flooding can destroy electronic equipment. The threats are numerous.

Outsourcing of IT operations represents other kinds of risks in addition to the threats mentioned above. All enterprises that outsource their IT operations have to trust a third party and its employees and systems. Outsourcing extends the social trust models of the organization. Important security risks include weak preparation before signing the contract, and weaknesses in the follow up management and the audit process. Market concentration and dependability on one provider also represent a risk. Dependability and lack of freedom shift the power from the buyer to the seller. Outsourcing across national borders implies more and other risks due to security responsibilities, differences in legislation and culture, geographic distances and secure communications.

After introducing the broad spectrum of threats, we can now turn to the NCCS06, which defines computer crime as "a legal offence in which a computer has been an object to fulfill an illegal act." The definition of computer crime is transformed to more practical and reportable incidents in the survey with notions as illustrated in Figure 3.1. The figure shows that the definition of computer crime and the subsequent definition of incidents cover only subsets of the potential incidents. Risks related to outsourcing are not included at all, neither are accidents. The juridical definition does not differentiate on motive. It does not focus on attack methods, such as use of insiders, and which weaknesses that were utilized. The emphasis of the survey is on threats utilizing vulnerabilities in software, as shown in Figure 3.1. Threats utilizing vulnerabilities in people, architecture and physical security is less emphasized.

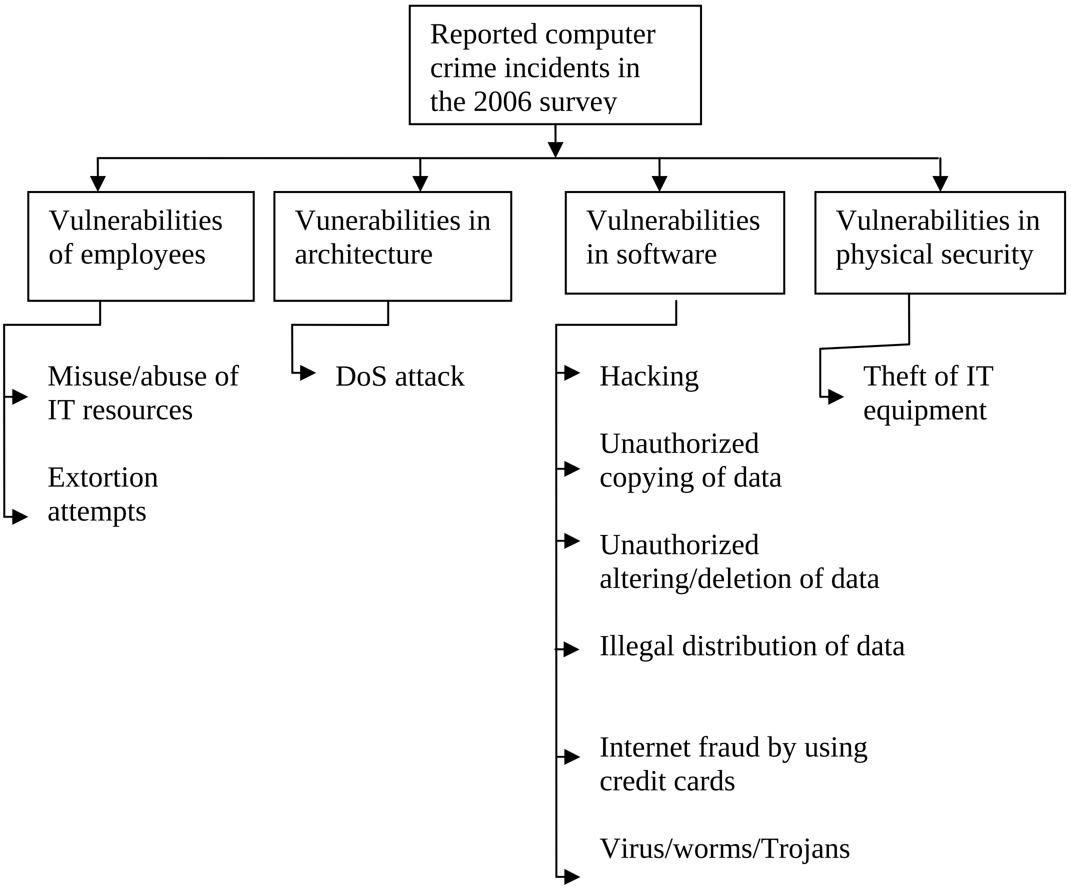
Reported computer crime incidents in the 2006 survey
Vulnerabilities of employees
Vunerabilities in architecture
Vulnerabilities in software
Vulnerabilities in physical security
Misuse/abuse of IT resources
Extortion attempts
DoS attack
Hacking
Unauthorized copying of data
Unauthorized altering/deletion of data
Illegal distribution of data
Internet fraud by using credit cards
Virus/worms/Trojans
Theft of IT equipment

Figure 3.1 Taxonomy of computer crime incidents

3.3.2 Security principles for defense of information systems

Defence in breadth and *defence in depth* are two well established security principles [24]. According to the defence in breadth principle you should be prepared to meet any threats. Therefore you should have a number of security measures implemented which cover different attack modes and systems. Defence in depth is also an important principle if the attacker penetrates the perimeter security. Some measures should be installed to detect and react to the attackers behind the perimeter security [37].

Security measures can be structured as proactive and reactive. *Proactive measures* can be defined as measures that prevent an incident to happen, or reduce the potential consequences of the incident. Proactive measures are preventive measures like passwords and user guidelines. It also includes emergency preparedness measures like backup of critical data and an emergency preparedness plan for what to do in a critical situation and how to run the business with fewer resources.

We define *reactive measures* as measures that react when the incident has occurred, aim to reduce further damage and secure evidence for the police. Reactive measures constitute intrusion detection systems and incident response measures exemplified by the process of reporting to the police.

Another approach to structuring security measures is to group them into *claim prevention measures* and measures that just aim to *reduce the consequences* when an incident arrives. From this perspective, it seems that both preventive measures and intrusion detection systems to some extent guard against undesired incidents and thus are claim preventive. One can argue that intrusion detection systems do not actively guard, but rather deter an aggressor from committing security breaches when he knows that they are installed. Emergency preparedness measures reduce the damage and consequences after incidents have occurred. Incidents response systems also help the organizations to handle the incidents and take lessons from them.

Applying this logic, we can sketch out the dimensions in a four fielded matrix as shows in Figure 3.2. These dimensions will moreover be used in the taxonomies presented in the next section.

	Claim prevention	Consequence reduction
Proactive approach	Preventive security measure	Emergency preparedness
Reactive approach	Incident detection	Incident response

Figure 3.2 A four fielded matrix for defense of information

3.3.3 Taxonomy for information security based on the questions of the Norwegian Computer Crime Survey 2006

We have developed taxonomies to visualize principles of good security practices and relate them to the data from NCCS06. Information security taxonomy is shown in Figure 3.3. We were inspired to develop the taxonomy by an enterprise security taxonomy presented in [1].

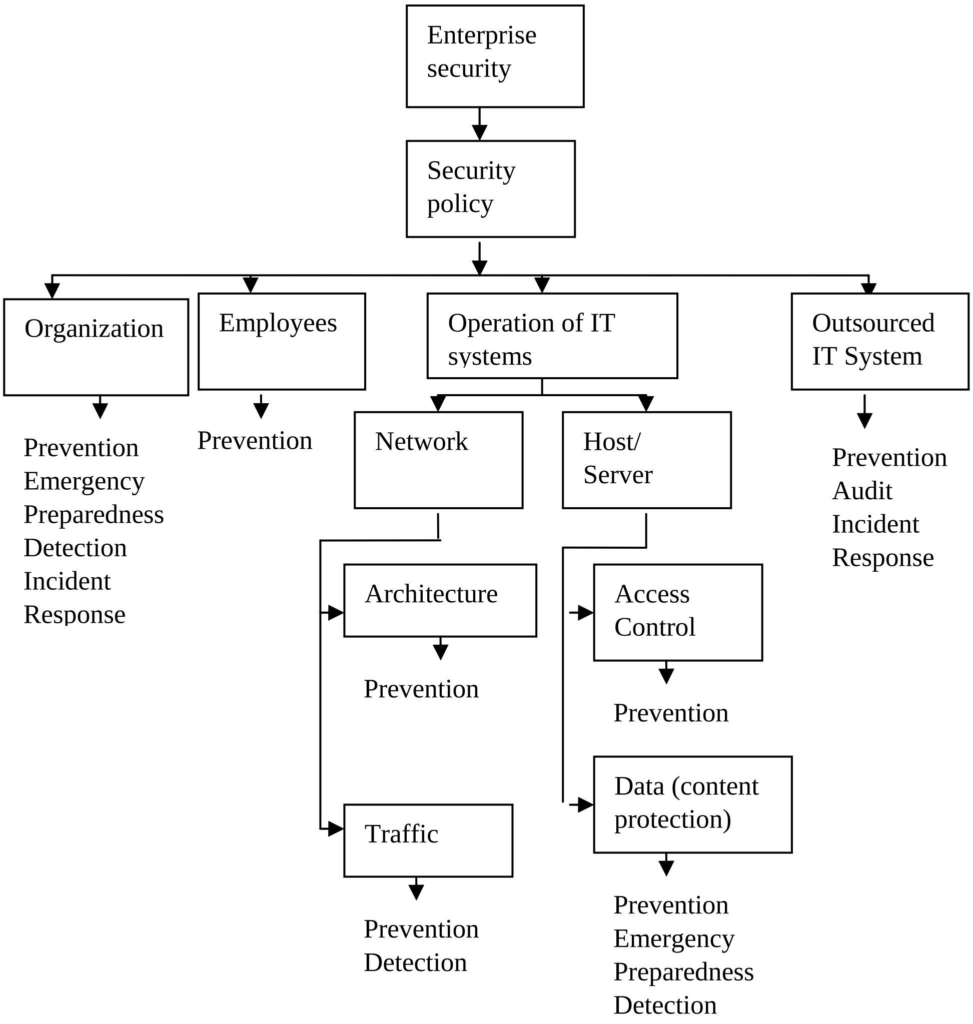

Figure 3.3 A taxonomy for the security measures in the computer crime survey

The security policy is considered to be the fundamental document [24] [36]. The security policy should be linked to the business strategy and outline the security requirements. The implemented security measures should correspond to the requirements in the policy. While the NCCS06 enquires into how security is implemented, it does not ask if the enterprises have a written security policy. Nevertheless, we have chosen to show the link between business strategies through the security policy further on to the implemented information security. The relation indicates that outsourcing security should be included in the overall security policy, as outsourcing and focusing on core businesses is a strategic decision.

We chose to separate enterprise security into four categories, representing a broad defense strategy which covers both technical and organizational security measures. The categories are:

- The organization as represented by formal procedures and systems, and the common attitudes and relations that tie people together into an organization.
- Humans will enter and leave an organization, and the employees are an important security factor and are hence located in one category.
- Operation of the IT systems can be handled in-house.
- Operation of the IT systems can be fully or partly outsourced to a third party.

Furthermore, we chose to divide operation of IT systems into the network level and the host/server level. Next, the network level was separated into one component of architecture and one component of traffic (content). Similarly, the host/server level was divided into access control and data (content) protection. Regardless of outsourcing model, the security measures should correspond to the requirement in the security policy, and all organizations should also have implemented organizational security measures and security measures directed towards their employees. Regarding network security and host/server protection, this may be fully or partly handled by the outsourcing partner, or by the enterprise itself. If operation of the IT systems is outsourced, the enterprise may need additional security measures to audit the outsourcing contract and services and react to incidents if the outsourcing partner does not deliver according to the contract.

By applying the taxonomy, security measures that were examined in the 2006 survey could be located in the taxonomy along the classic defense-in breath and defense-in-depth dimensions. Applying the taxonomy makes it easier to evaluate the security practices and draw conclusions on the protection strategy profiles of the enterprises that have answered the questionnaire compared to the traditional way of reporting security practices.

3.3.4 Security measures at organizational and individual levels

The organizational measures and the measures directed towards the employees addressed in the survey are located in the taxonomy as shown in Table 3.3.

Table 3.3 Organizational measures in the survey at the organizational and individual level

	Organization	**Employees**
Prevention	Risk and vulnerability analysis of existing IT systems	User guidelines
		Non-disclosure agreements
	Risk and vulnerability analysis of new IT systems	Educating employees in information security
Emergency preparedness	Plans to manage security breaches	
	Systematic IT exercises[7]	
Detection	Internal audit control	
	External audit control	
	Analysis of logs	
Incident response	Ability to manage security breaches outside working hours	
	Reporting to management	

As the employee directed measures focus solely on prevention, the organizational measures conserve the organization's ability to stay in all phases of the defense-in-depth strategy. It should however be commented that depending on the content of the education, employees can become both detection capabilities and resources in an emergency situation. The survey does not address these questions.

3.3.5 Technical security measures at network and host/server level

Technical security measures are located in the taxonomy as shown in Table 3.4. By matching the security measures in the survey with the taxonomy, it becomes apparent that the technical security measures addressed by the survey do not cover all stages in the defense-in-depth strategy. The addressed technical measures have a strong focus on intrusion prevention. Emergency preparedness is provided by backup, and detection capabilities are given by antivirus software and intrusion detection systems. To go through with the defense-in-depth strategy, one could have included, for instance, questions about the use of technical forensic tools.

[7] Internal and external control is used to follow up the user guidelines.

Table 3.4 Technical measures in the survey at network and host/server level

	Network		**Host/server**	
	Architecture	**Traffic control**	**Access control**	**Saved data**
Prevention	Duplication of critical components	Network firewall	Personal password	Personal firewall
	Separated network security zones	Spam filter	One time passwords	Encrypted portable IT equipment
	Encryption of wireless network	Filtering unwanted network traffic	Physical authentication	Digital signature
	Virtual Private Network (VPN)	Auditing the firewall rules	Biometrics	
		Patching security software	Access control reviews	
			Updating OS Administrator passwords Locked server room	
Emergency preparedness	Backup power supply			Backup power supply Backup
Detection		Intrusion detection system (IDS)		Intrusion detection system (IDS) Antivirus software

3.3.6 Outsourcing and security of IT operations

The enterprises in the survey that have outsourced parts or all of their IT operations can apply a defense-in-depth strategy in the outsourcing contract. This could be done at three levels:

1. Initially it is important to produce a well-defined contract. This can be achieved by including security requirements covering routines and mechanisms for access control to enterprise critical information, requirements regarding use of security technologies, and routines and requirements with respect to the availability of systems.
2. Secondly, a detection capability regarding compliance with security requirements could be achieved through auditing and security reviews or measurements.
3. Finally, the last line of defense concerns reducing the consequences of security breaches by liability for compensation and sanctions.

Figure 3.4 shows the taxonomy for outsourcing.

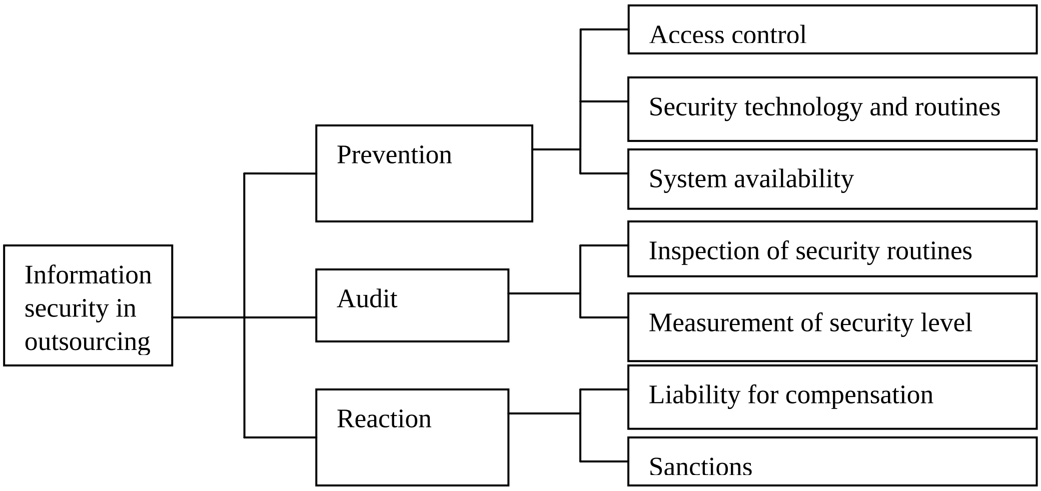
Information security in outsourcing
Prevention
Audit
Reaction
Access control
Security technology and routines
System availability
Inspection of security routines
Measurement of security level
Liability for compensation
Sanctions

Figure 3.4 A taxonomy for security in outsourcing contracts

3.4 Statistical methods to measure the effectiveness of security measures

We assume that enterprises invest in security for two reasons; to reduce the risk (number of incidents and economic losses) and to increase the return of investment. Because the survey collects data on these variables, in addition to the mapping of security practices, it is possible to conduct correlation analysis on these variables.

Do enterprises that have implemented many security measures report fewer incidents, less losses, and higher financial returns compared to those that have invested less in security measures? This research question is answered by testing H_0 (0 hypothesis):

There is no correlation between security measures and reported undesired incidents/economic performance.

First, after plotting the data, we removed outliers in the data set. Outliers were detected by sorting the reported number of the ten categories of computer crime incidents in the survey. 13 cases were deleted in order to remove outliers[8].

Then, we applied factor analysis with varimax rotation to the large number of technical and organizational security measure variables addressed in question 12.A and 13 in the questionnaire. These binary questions were answered by all enterprises in the survey. The factor analysis is applied in order to achieve a more manageable number of independent factors that can be used in subsequent analysis. The factors are reliability tested and furthermore adjusted to satisfy a requirement of Cronbach's alfa >0.7. Cronbach's alfa is the squared correlation between the observed score and the true score. The values are between 1 and 0; the higher the value, the

[8] Cases numbered 160, 413, 551, 71, 663, 97, 12, 328, 583 and 395 were deleted from the data set. In addition, the cases numbered 499, 612 and 358 were also deleted because of their clear deviant economic performance.

better. The security measures included in each adjusted factor are then transformed to an index with values between 1 and 0. This is done by calculating the average score value of the measures included in the factors. These indexes are used in subsequent analysis as independent variables.

Spearman correlation analysis was then applied on the independent variables (the security measure indexes) and on the dependent variables (the total numbers of reported incidents and economic performance). Economic performance is measured as registered economic return before tax and reported economic loss due to computer crime incidents.

For all hypothesis testing and application of Spearman correlation analysis, we required a significance level of 5%. Because we did not know the direction of the correlation, we applied a two-sided test. We chose Spearman correlation because Pearson's correlation coefficient is a measure of linear association. Two variables can be perfectly related, but if the relationship is not linear, Pearson's correlation coefficient is not an appropriate statistic for measuring their association. Spearman requires linear relationship between the ranks. In addition Spearman is less sensible for outliers, and a more robust alternative. We also excluded “cases list wise”. This means that cases with missing values for any variable are excluded from all correlations.

The next step was to refine the dependent variables by adjusting them according to the size of the enterprise measured by the number of employees. This was done in order to compensate for potential underlying factors like economies of scale, and to address the fact that large enterprises may be more exposed to security incidents because they have more users and more complex systems, or are more attractive targets because of their position and resources. Therefore we calculated the average number of incidents, the average return of investment and average economic losses of computer crime per employee. Spearman correlation analysis was applied to the security measures indexes and these new dependent variables.

Finally, a linear regression analysis was conducted with derived security indexes as independent variables and the following dependent variables: the number of reported incidents, return of investment and reported economic losses.

All statistical analysis is conducted by the help of the statistical software SPSS.

4 How vulnerable are Norwegian Enterprises for outages in Internet services and how serious are the consequences of the reported computer crime incidents?

4.1 Use and dependency on Internet services

The more dependent the enterprises are on Internet services, the larger are the expected losses of computer crime. Use of IT and Internet services is presented in Figure 4.1.

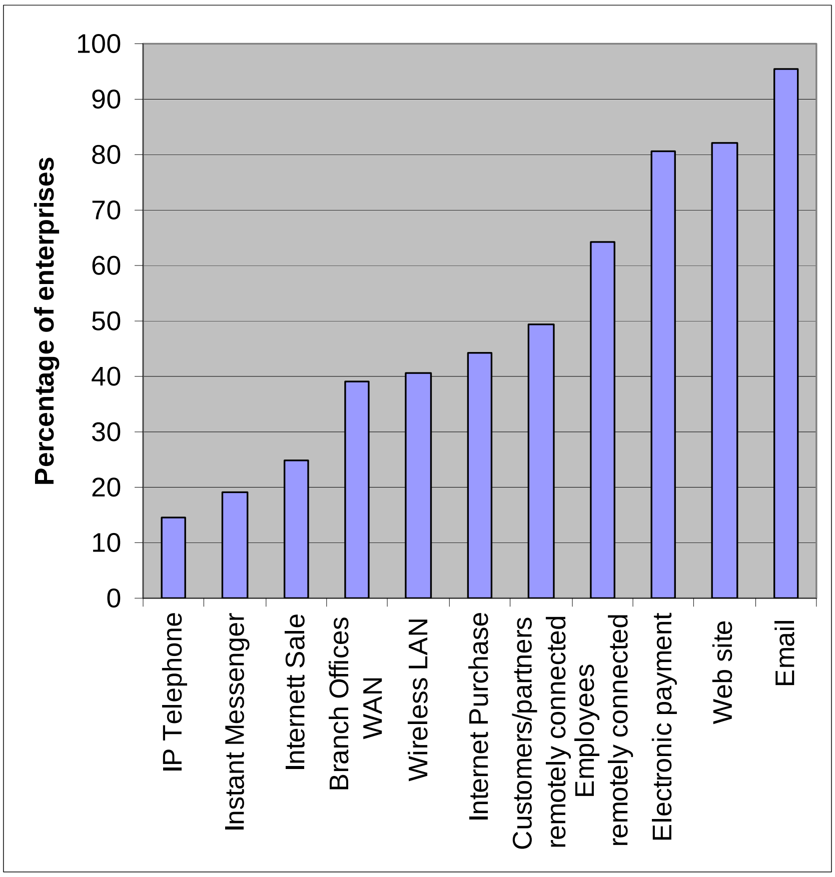

Figure 4.1 Utilization of various Internet services

The data shows that more than 80% of the enterprises depend on the Internet in business processes such as business communication through email, promotion and/or trade by web sites, and electronic payment on the Internet. While electronic payment on the Internet and email are widely adopted by all kinds of enterprises, web sites and other Internet services are more commonly used by the larger ones. The use of new communication technologies like wireless networks and instant messenger is increasing.

Critical infrastructure enterprises make more extensive use of Internet services compared with ordinary businesses. This finding is not surprising because the critical infrastructure enterprises are dominated by large enterprises, which hold a leading position in adopting new technologies.

A major share of large enterprises and enterprises belonging to the group “critical infrastructures” offer employees, customers and partners remote connections to the enterprise IT systems. While only 35% of the small enterprises with fewer than 10 employees offer the employees remote system connections, the corresponding number for larger enterprises with more than 200 employees is 91%. Looking at similar numbers for critical infrastructure enterprises, the results show that 73% of the enterprises offer remote connections, compared to 64% in other businesses. Customers and partners are to a lower degree offered remote connections. Less than 30% of the small enterprises with fewer than 10 employees offer customers/partners remote system connections. The corresponding number for larger enterprises with more than 200 employees are approximately 70%. Looking at critical infrastructure enterprises, 57 % of the enterprises offer remote connections, compared with 48 % of other businesses.

In 2006, wireless network (WLAN) is used by 41% of the enterprises, an increase of about 30% since 2003. IP telephone services have not shown a similar development yet. Only 15% of the enterprises use IP telephony in 2006. There has also been an increase in remote connections to IT-systems for employees, from 43% in 2003 to 64% in 2006. Internet trade has also increased from 9% in 2003 to 25% in 2006. The growth is probably even higher because of the change in composition of enterprises in the samples: the 2006 survey sample included a higher number of small enterprises than the 2007 survey sample. These observations show that Norwegian enterprises are expanding their use of IT Internet services. Foreign computer crime surveys do not map the usage of Internet services.

The wide usage of Internet services documents that the Internet has been integrated into important business processes. A majority of Norwegian enterprises, small and large, are therefore dependent on the Internet. In the case of a 24 hours outage of critical Internet services, as much as 70% of the enterprises report to face huge problems. After 2-3 days, as much as 90% of the enterprises have problems to do business. Figure 4.2 provides more details on duration of service outages and their business consequences.

Comparing the findings of the 2006 survey to the Norwegian Computer Crime Survey 2003, a tendency pointing to growth in critical dependency on the Internet appears. In 2003, 15% of the enterprises reported that they would suffer seriously from one hour outage of Internet services; in 2006 this has doubled to 31%. The finding corresponds to the increase in use of Internet services. None of the foreign surveys address the time dependency the way the Norwegian survey does.

The dependency is expected to further increase as new technological solutions enter the market. Mobile telephones with operating systems and ability to synchronize against your computer will provide increased usability, but also require security measures. Moreover, we can expect that future shareware solutions will improve usability, but also imply other security challenges.

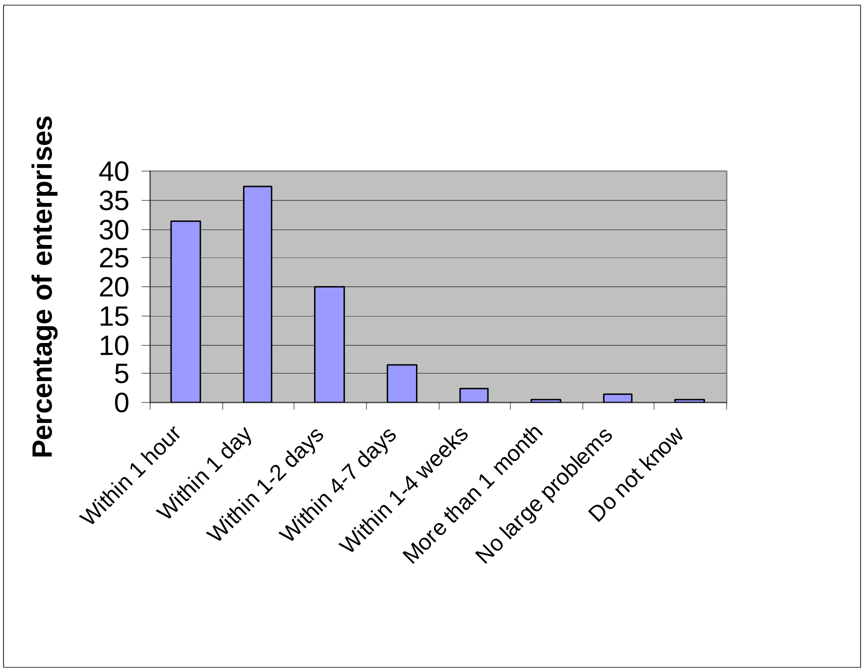

Figure 4.2 Duration of service outages and their business consequences

Summary:

- More than 80% of Norwegian enterprises depend on the Internet in critical business processes, such as business communication, promotion and payment.
- As much as 70% will have huge problems to do business if Internet services are out for a day, as the Internet has been integrated into important business processes.

4.2 Reported computer crime incidents and consequences

The number of reported computer crime incidents in the survey are presented in Table 4.1 and organized according to the taxonomy, see Figure 3.1. We observe that the number of real malware infections surpasses the number of all other reported incidents in the survey. After malware infections, theft of computer equipment is most common. It must be emphasized that outliers are included in the reported statistics. What to do with the outliers were discussed at one meeting of the Computer Crime Committee, and the committee decided to include the cases that reported exceptional large number of incidents after comparing the findings with previous surveys and discussing the findings with Perduco. This decision has later been criticized in a master thesis at Gjøvik [29]. The author emphasized that if the outliers were excluded, the total number of computer crime incidents would be reduced from 2079 to 1386, hence reducing the dark numbers. She also argued that the outliers were typing errors and should not be included at all. Including or excluding outliers affects the numbers of malware infections, DoS attack and hacking. Removing the outliers change the internal ranking of the top three threats from 1) malware infections, 2) theft of IT equipment and 3) hacking to 1) malware infection, 2) theft of IT equipment and 3) IT-misuse.

If we add this uncertainty to the challenge of detecting computer crime incidents, it becomes apparent that the reported incidents, at best, provide an indication. This is also one of the challenges of using these answers for further analysis.

Table 4.1 The number of reported computer crime incidents sorted according to the taxonomy

Taxonomy category	Computer crime incidents	The number of reported incidents during last 12 moths	Number of responses (N)
Individual	Misuse/abuse of IT resources	94	493
	Threats to attack the IT systems (extortion attempts)	33	537
Architecture	DoS attack	149	493
Software	Hacking	226	532
	Unauthorized copying of data	7	506
	Unauthorized altering/deletion of data	88	516
	Illegal distribution of data	13	495
	Internet fraud by using credit cards	31	547
	Viruses, worms and Trojans	1118	534
Physical security	Theft of IT equipment	320	587
All categories		2079	

If we then study the percentages of enterprises attacked within each computer crime category, we see that malware infection and misuse/abuse is the most common computer crime incidents. From this comparison we can also observe that those enterprises that have reported theft of data equipment, have reported several theft incidents. Those reporting misuse/abuse report fewer incidents per enterprise.

Table 4.2 Percentage of enterprises that have reported incidents

Taxonomy category	Computer crime incidents	Percentage of enterprises	Number of responses (N)
Individual	Misuse/abuse of IT resources	8.8	493
	Threats to attack the IT systems	0.6	537
Architecture	DoS attack	4.6	493
Software	Hacking	3.9	532
	Unauthorized copying of data (theft of data)	1.2	506
	Unauthorized altering/deletion of data	5.2	516
	Illegal distribution of data	1.6	495
	Internet fraud by using credit cards	1.3	547
	Viruses, worms and Trojans	35.2	534
Physical security	Theft of IT equipment	26.1	587
All categories			

The 2005 FBI Computer security Survey [2] and the Australian survey [11] show a higher percentage of attack (virus infection and theft) compared to the Norwegian survey even when outliers are included. One possible explanation is that larger organizations have more users and complex networks, and are thus more exposed. What are the consequences of computer crime incidents? The Norwegian survey measures the consequences as time to restore the system after an attack. The results in Figure 4.3 show that threats, illegal distribution of data and theft of computer equipment have the most serious consequences, which was also most costly to recover from.

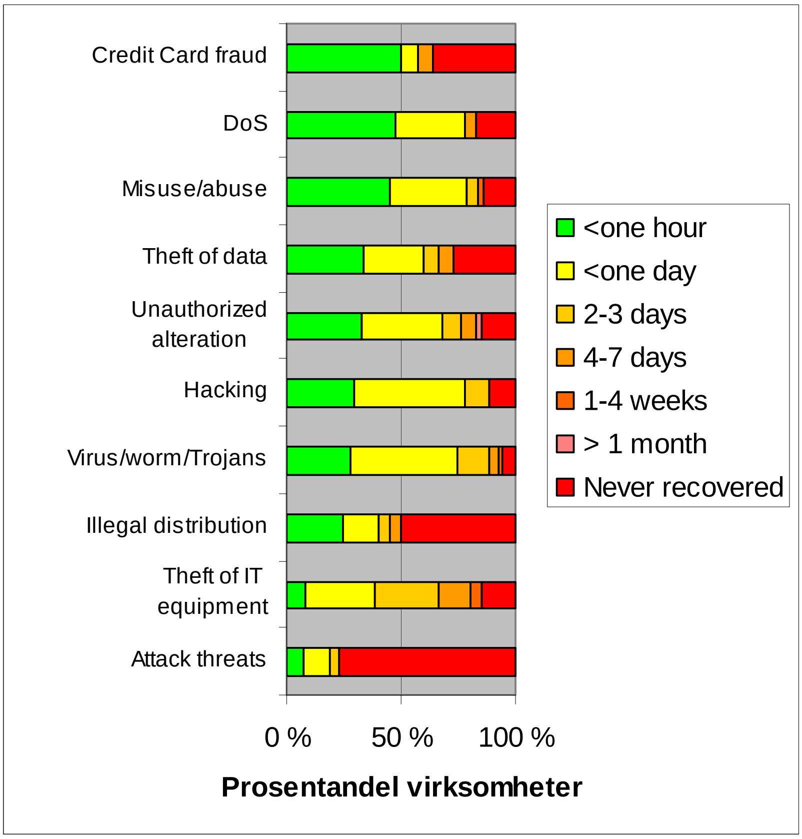

Figure 4.3 Consequences of different computer crime incidents – time to recover

Figure 4.4 shows that the majority (67.2 %,) of the enterprises reported extra work as a consequence of computer crime incidents. As much as 28.9% did not report consequences at all. Loss of reputation is reported by just 0.6% of the enterprises that answered the question. This is very low in contrast to the findings of foreign surveys [11][12].

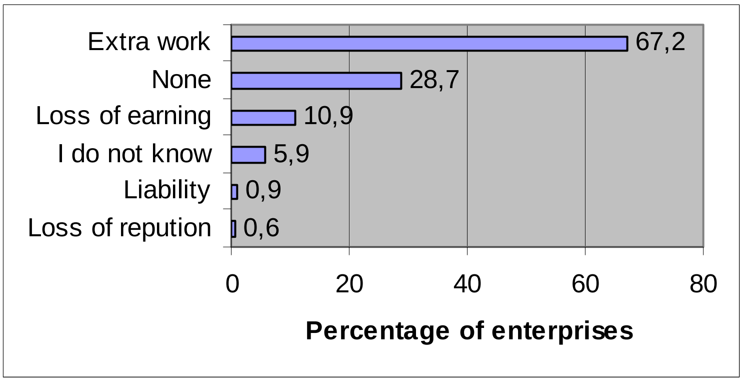

Figure 4.4 Consequences of computer crime incidents, multiple answers (N=341)

Studying the economic consequences, the data shows that few enterprises report huge losses. The Norwegian losses are small compared with losses documented by foreign studies. As much as 55% of those answering the question on economic losses report to have no economic losses at all.

Table 4.3 Economic consequences: costs and losses (N=209)

Cost interval	Percentage of enterprises	N
No costs or losses	55,5	116
1000-9999 NOK	9,1	19
100000-19999 NOK	7,7	16
20000-39999 NOK	9,6	20
40000-59999 NOK	10,5	22
60000 NOK	7,7	16

Table 4.4 shows the number of responses to the questions about perpetrators and how many times the perpetrators were detected. We see that own employees constitute a considerable contributor to computer crime incidents. Also consultants are a risk factor. But the high number of unidentified perpetrators also illustrates the difficulties in identifying and catching the perpetrator.

Table 4.4 Who are the perpetrators?

Perpetrator	Number of times the perpetrator were detected	Number of responses (N)
Own employees	155	116
Consultants/service	26	19
External	220	101
Unknown	448	169
Total	849	

Summary:

- Due to large uncertainty in the reported numbers the reported incidents provide an indication rather than an exact answer. Malware infection and theft of IT-equipment are the two most common incidents reported in the survey, even when outliers are removed.
- It is difficult to identify the perpetrator when security breaches are detected. When identified, insiders are a significant threat although external actors dominate.

- The reported economic losses are low. 30% of the enterprises that answered the question on consequences of computer crime incidents reported no consequences at all. The most frequently reported consequence is extra work.

4.3 Incident reponse and learning

A holistic approach to security requires incident response capabilities and a learning process. What do the enterprises do, when becoming vicitms of computer crime? We can conclude that very few calculate the costs of crime. Only 11% of the infected enterprises have routines for calculating the losses due to computer crime. This makes the estimates of total economic losses unreliable. In addition, it makes it difficult to document the losses and require any compensation, see Section 3.3.6. The majority of the incidents are handled with own resources. External assistance is requested mainly for malware infection. Also, only a small part of all computer crime incidents are reported to the police, see Table 4.5. There are, however, two exceptions: Incidents of theft of data and computer equipment are reported to the police at a rate of, respectively, 100% and 73%. Theft of data is a rare incident, but is expected to have huge consequences for the enterprises. When IT equipment is stolen, the insurance companies may require that the theft is reported to the police before they cover the losses.

Table 4.5 Serious incidents that are handled by experts or reported to the police

Taxonomy category	**Computer crime incidents**	**Percentage of incidents where experts were called**	**Percentage of incidents reported to the police as a criminal offence**
Individual	Misuse/abuse of IT resources		
	Threats to attack the IT systems (extortion attempts)	4	7.4
Architecture	DoS attack	4.4	0.7
Software	Hacking	6.4	1.3
	Unauthorized copying of data (theft of data)	0.9	100
	Unauthorized altering/deletion of data	2.5	2.3
	Illegal distribution of data	0	0
	Internet fraud by using credit cards	0	71
	Viruses, worms and Trojans	29.9	0.1
Physical security	Theft of IT equipment	10.3	73.1
All categories			2079

227 enterprises answered the question about why they did not report the incident to the police. Almost half of these didn’t report the incident because they regarded it as unimportant. 35% did not report the incident because the attack was not directed towards the enterprise, and 22% because it was too resource demanding.

What initatitives do the enterprises after experiencing computer crime incidents? Improvement of security routines was the most frequently taken initiative, followed by investment in security technologies. 14% performed a total security review to find solutions. It is worth noting that 22%

took no initiatives. Table 4.6 shows that detecting computer crime incidents lead to improvements in security for the majority of the infected enterprises. This illustrates the utility of detecting incidents and that detecting incidents also leads to improvements in security.

Table 4.6 Initiatives after detecting computer crime incidents, N=314

Initiative	Percentage of enterprises
Improving routines	43,9
Security technologies	38,9
Nothing	22,3
A total security review	14,3
Do not know	4,8
Strengthen security personnel resources	4,1

Summary:

- Those reporting incidents handle the incidents by own resources; very few report computer crime to the police as a criminal offence and few engage experts.
- Approximately 1 of 10 enterprises has routines to calculate the economic losses of computer crime, and the majority of enterprises have therefore limited ability to document the losses.
- After detecting an incident, the majority improve the security system.

5 Which security measures have Norwegian enterprises implemented to mitigate computer crime and how does this practice correspond with good security principles?

5.1 Implemented security measures against computer crime

5.1.1 The employees and the organization

Information security is not limited to technical issues. No preventive measures can provide adequate security assurance, unless the organization also has an effective strategy for handling intrusion dynamics that include preparation, detection and response. Also, the employees must be aware of their responsibilities for security, as the success of an information security program is dependent on the commitment of all employees. If not, the security mechanisms could be circumvented fully or partly by the employees [28]. Security measures directed towards the employees, as presented in the taxonomy in Table 3.3, have therefore been examined in the 2006 survey. The results are shown in Figure 5.1. User guidelines are most common: 65% of the enterprises have user guidelines for secure IT use. Non-disclosure agreements are used by 43% of the enterprises. Studying these measures, the trend is still that large enterprises and enterprises within critical infrastructures perform better than small ordinary enterprises. Few enterprises (40%) educate their employees in secure use of IT and the Internet. The differences in education practices among types and sizes of enterprises are, however, insignificant. These three questions on organizational security measures are new in the 2006 survey. Foreign surveys are also concerned with awareness raising. According to the UK survey [10] defining security rules that the staff must follow is a foundation for proper security management. The Norwegian results correspond to the UK findings: 35% of UK businesses make its employees aware of the security rules through training or presentations, compared to 40% of the Norwegians. The result suggests that there is room for improvements.

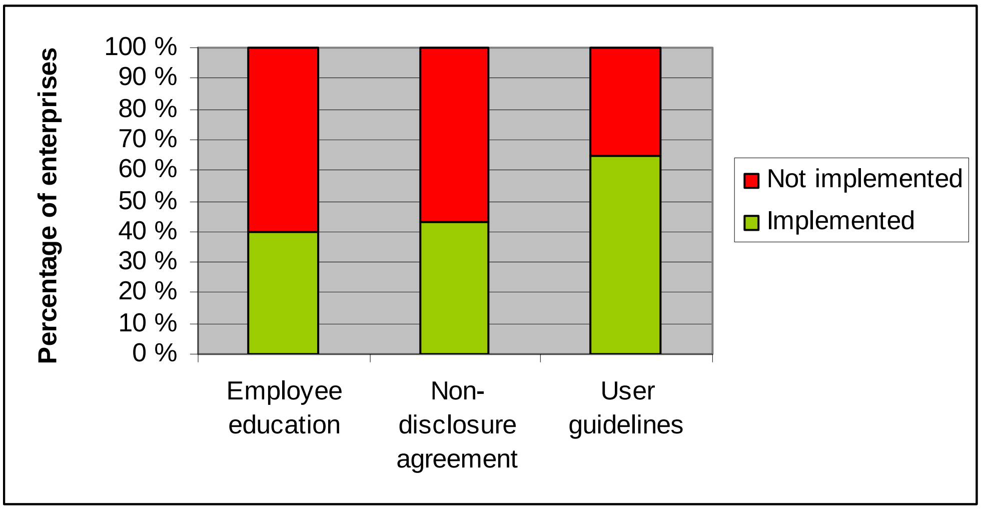

Figure 5.1 Preventive measures for the individuals in the enterprises, N=749

The measure to carry out risk analysis of new and existing IT systems is defined within the frame of preventive organizational security measures, as shown by the taxonomy in Table 3.3. A risk analysis does not actively prevent intrusions, but enable the management to apply a risk based management approach and decide on the security investments. In a dynamic world and through mergers and acquisitions, risk analysis provides information on altering threats and vulnerabilities. The 2006 survey asked questions about risk analysis frequency as shown in Figure 5.2. The result shows that for those enterprises that have guidelines for secure IT operations, risk analysis is carried out more frequently in new systems compared to existing systems. Studying the data in more detail, larger enterprises and enterprises within critical infrastructure perform better on this issue than smaller and ordinary enterprises. The question is new in 2006 survey, and foreign computer crime surveys did not address similar questions.

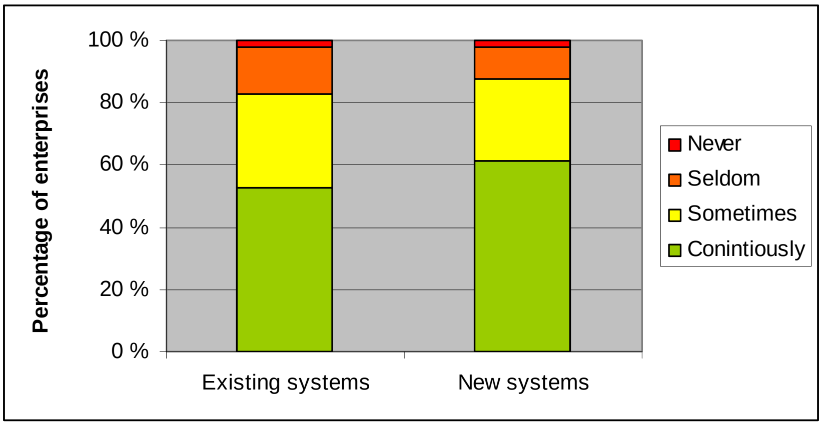

Figure 5.2 Risk analysis frequencies of existing and new systems, N=584

Moving one step further in the defense-in-depth strategy, the emergency preparedness dimension addresses two questions: (1) Plans to manage security breaches and (2) systematic IT exercises. Both the plans and the exercises are important to prepare for emergency situations and reduce the undesired consequences, and these two measures can be implemented in advance before an emergency situation occurs. Few enterprises, however, have implemented emergency preparedness measures. The results show also a gap between the two measures: 26% have plans, and only 9% perform exercises, se Figure 5.3. Larger enterprises have these measures in place more frequently compared to smaller enterprises. More than 50% of the enterprises with 200+ employees have plans in place; correspondingly 19% have systematic exercises. Similarly, these two measures are more common among the critical infrastructure enterprises than among ordinary enterprises. In contrast, the UK survey [10] reveals that 58% have disaster recovery plans in place and 26% have tested their plan during the last year.

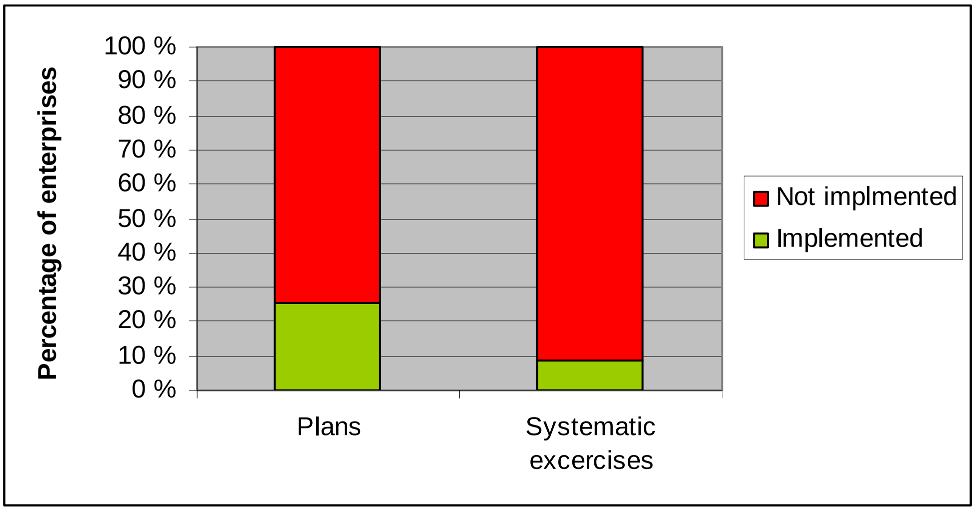

Figure 5.3 Emergency preparedness by plans and exercises, N= 749

The enterprises were asked how they followed up their guidelines for secure IT operations. Internal and external audit controls are two relevant methods that were examined in the survey. The results show that 52% of the enterprises that have such guidelines perform internal audit controls, while 26% of them perform external audit control, and engage third parties in the auditing process, see Figure 5.4. The trend shows that large enterprises and critical infrastructure enterprises perform much better than smaller and ordinary enterprises.

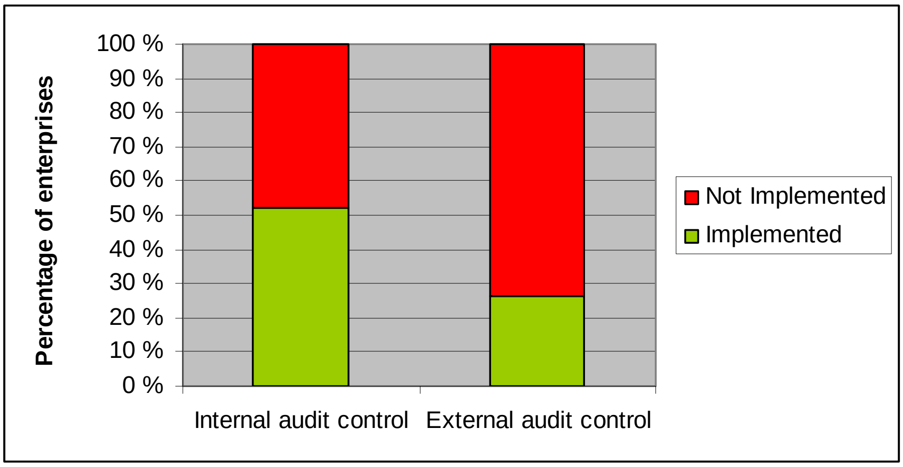

Figure 5.4 Detection by audit controls, N= 584

Analysis of logs is also a way to detect alterations in IT use and track incidents. In average, 15% check the logs daily and 13% weekly. Figure 5.5 visualizes the trend that larger enterprises perform better than smaller ones. In general 20% of the enterprises do not log or check the logs afterwards.

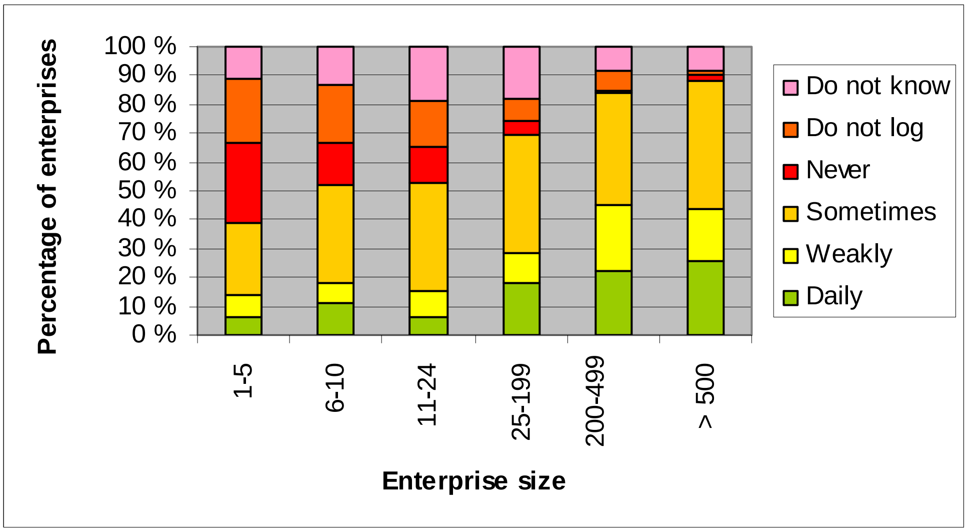

Figure 5.5 Log check frequencies, N=732

Compared to an American survey, which documents that 35% of American enterprises do not log [2], the Norwegian enterprises perform better; only 11% answer that they do not log. A comparison with the 2003 survey [3] shows a decline, but that can partly be explained by a change in the structure of the sample, which in 2006 had a higher number of small enterprises.

Through the Internet, customers can reach Internet shops that offer around-the-clock opening hours (24 hours/7 days a week). While the e-businesses have developed around-the-clock opening hours, the majority of the enterprises still do not have around-the-clock security incident response capability. In average, 38.5% of the 749 enterprises in the survey claim to have the ability to manage security breaches outside working hours.

Among the enterprises that have incidents reporting routines (N=569), 54% claim to report security breaches and incidents immediately to the management, see Figure 5.6. Periodic reporting is practiced by 14% of the enterprises. Small enterprises report security incidents immediately to management more often compared to larger enterprises, which more frequently seem to a have routines for periodic reporting. Only 12% do not report incidents at all. One possible explanation of these findings is that larger enterprises more often have formalized systems and a security organization than the smaller enterprises. In the smallest enterprises, with less than 25 employees, the top executive is responsible for security issues directly. In the large enterprises, with more than 500 employees, the responsibility lies with a security chief executive.

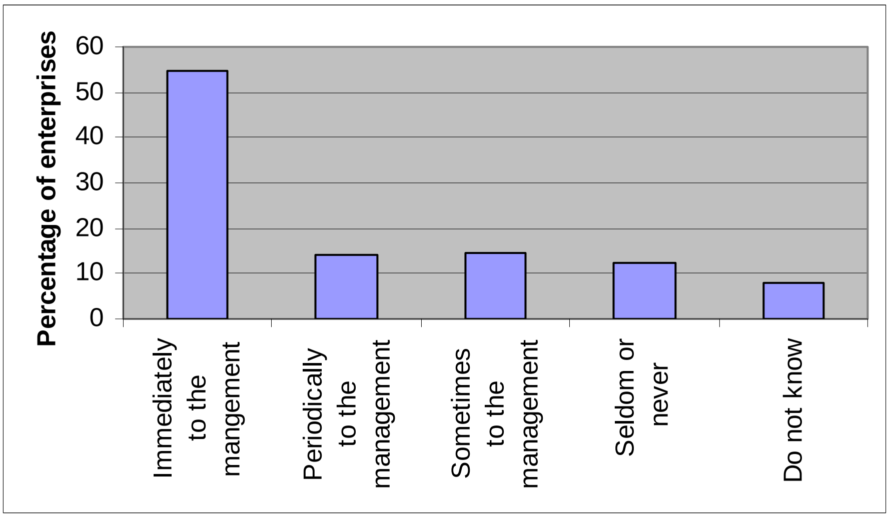

Figure 5.6 Internal incidents reporting procedures, N=569

Summary:

- Formal security measures, such as user guidelines and non-disclosure agreements, are most commonly employed: 65% and 43% of the enterprises have taken such measures.
- Education of employees is provided by 40% of the enterprises. Here is no significant difference between large and small enterprises.
- Norwegian enterprises are poorly prepared for an emergency situation: less that 30% have implemented emergency plans and exercises.
- Incidents are mostly reported immediately to the management. The reason for this is that the majority of the enterprises in the survey are small ones with more informal organization and shorter distance to top management, compared with large enterprises with more than 500 employees.
- According to good security practices, the enterprises should pay more attention to education and security throughout the defense in-depth-chain.

5.1.2 Protection at the host/server level

The purpose of access control measures is to prevent unauthorized access to IT resources. They consist of logical and physical measures and include personal passwords, one-time passwords, physical authentication (e.g. tokens and smart cards) and biometric authentication. These measures can be both complementary and alternative to each other. Typically stronger access control can be achieved by multi-level authentication: something you know (password), something you have (smart cards) and something you are (biometrics). It is also important to control the physical access to servers, because malware can be installed easily by use of physical means like CDs and memory sticks. Servers should therefore be protected in restricted areas/locked rooms. The survey shows that the use of personal passwords is widespread among all enterprises. One may conclude that traditional password authentication still is a central factor for security in Norwegian enterprises of all sizes, see Figure 5.7. The quality of this security measure depends on the passwords' strengths. For all preventive access measures, there is a tendency that the use of a variety of access control mechanisms increases with enterprise size. We also see that just 26% report using physical locks for server rooms. There are significant differences between large and small enterprises; roughly 90% of the enterprises with at least 200 employees have locked server rooms, in contrast to 10-20% of the enterprises with less than 25 employees.

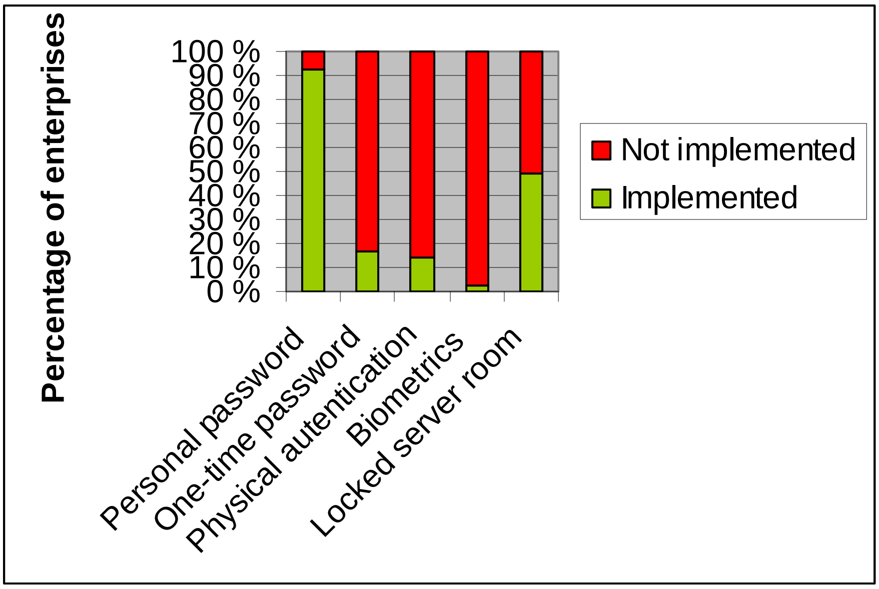

Figure 5.7 Access control measures, N=749

Frequently updating the access controls and changing the administrator password are additional means to restrict unauthorized access. These measures are complementary to the access control measures and physical security, as presented above. Figure 5.8 visualizes the practices regarding review of access controls and administrator passwords. The figures reveal that the majority review the access controls (N=680) and change administrator passwords (N=684) at least yearly. Studying the data in-depth, we see that while more than 80% of the large enterprises with more than 500 employees perform a review at least yearly, this rate drops significantly the smaller the enterprise is.

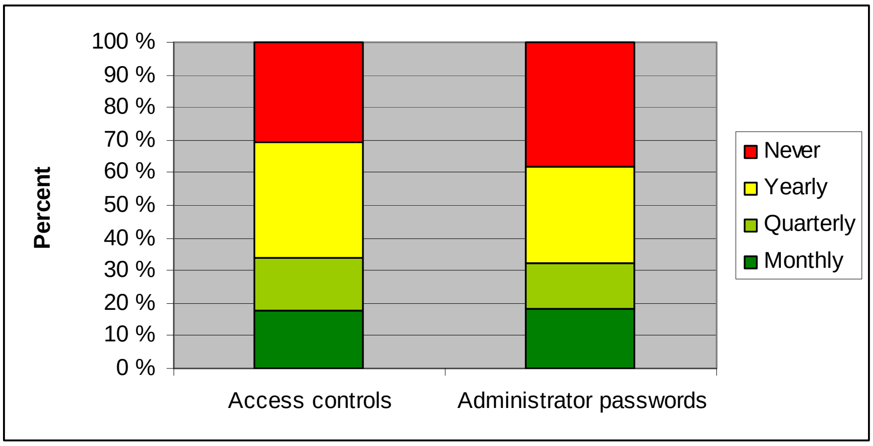

Figure 5.8 Frequency of reviews of access controls and administrator password, N=680/684

The frequencies for patching the operating system (OS) are shown below in Figure 5.9. Security patching routines can be automated or manual. The result shows that almost 70% of the enterprises perform updates occasionally or regularly. 90% of the large enterprises update OS periodically, when patches are released, or automatically.

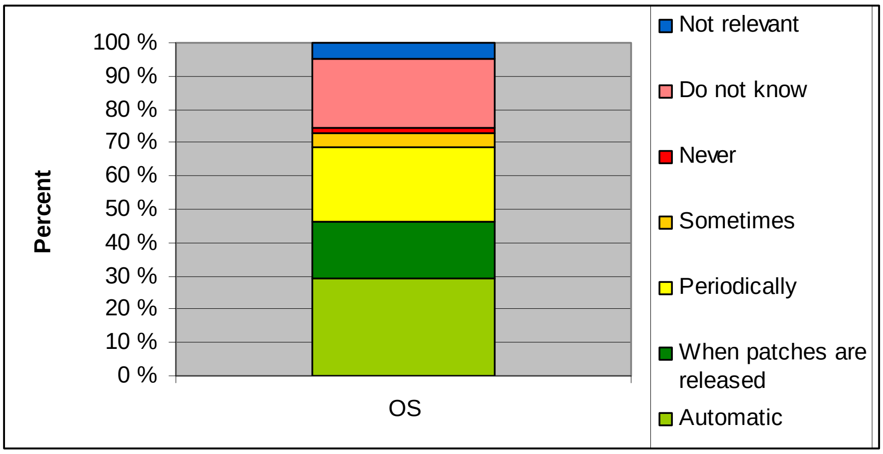

Figure 5.9 Patching frequencies for updating the operating system (OS), N=640

If the authentication and access control are compromised, the data that are stored on a PC or server can be protected by other preventive techniques. A firewall restricts non-permitted traffic access. Encryption of portable IT equipment, for instance laptops, provides confidentiality of the data. A digital signature confirms the identity of the sender, and ensures that the message in not altered on its way to the recipient. These are all complementary security measures in a security regime.

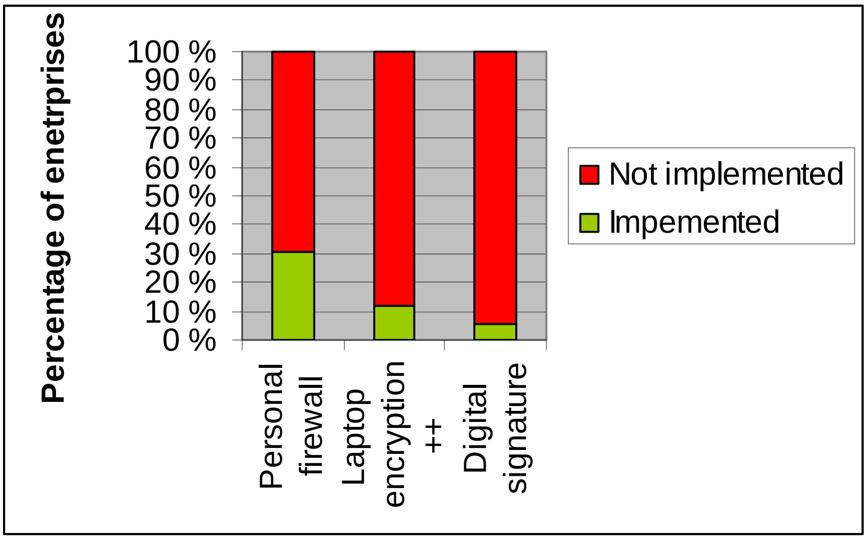

Figure 5.10 Protection of stored data, N=749

The results show that these measures are rarely employed, see Figure 5.10. The use of personal firewalls is the most widespread measure among enterprises of all sizes: 31% of the enterprises have personal firewalls, an increase from 16% in 2003. Only 12% have encrypted laptops and other portable IT equipment, and digital signature is hardly used at all. In contrast, the UK survey [10] reports that 36% use public key infrastructure (PKI). Studying the Norwegian data further, we see that there is also a clear tendency that large enterprises implement more and a wider range of such measures.

Emergency preparedness measures include backup power supply and backup of data. The measures ensure the availability of data in case of power outages, or system or data crash. The results show that the majority of the enterprises have implemented systems for data backup (89%), while fewer have invested in power supply backup (65%), see Figure 5.11.

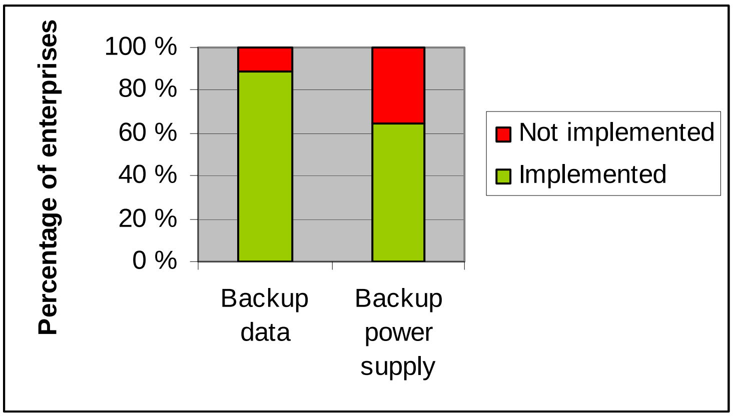

Figure 5.11 Backup power supply and data, N=749

Intrusion detection and antivirus software are both measures aiding the detection of intrusions. While the majority report to have anti-virus software installed, a minority (16%) of the enterprises have invested in intrusion detection systems (IDS), a slight increase from 11% in 2003, see Figure 5.12. Antivirus software is well distributed among all enterprises, but IDS is mainly used by the larges ones (with more than 200 employees). In contrast, 69% of the respondents of the “2006 CSI/FBI Security Survey” [9] report to use IDS. It should be noted, however, that this survey also includes a higher number of large enterprises.

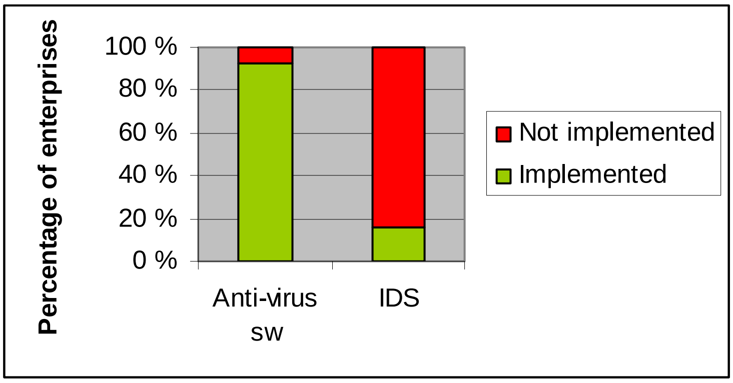

Figure 5.12 Detection mechanisms, N=749

Summary:

- Use of personal passwords is the most widespread preventive measure for protection against unauthorized access; it is important that good practices are followed for password generation and password administration to ensure security, also multi-level authentication can improve the security.
- Backup of data is the most important emergency preparedness measure.
- Antivirus software is the most frequently used measure enabling detection of intrusion and malware attacks.
- There is a clear tendency that large enterprises have implemented more security measures compared with small enterprises.
- Encryption of data and use of digital signature is not widely applied at enterprise level.
- Mature security technologies are more widely adopted than newer security technologies like biometrics.

5.1.3 Network security

The network security dimension includes architecture and traffic control. The security measures addressed in the survey are mainly preventive. Backup power supply and IDS are relevant, but these measures are commented on in the previous section, and will not be discussed here.

First, the results show that network security measures are applied among less than 50% of all the enterprises (Figure 5.13). Among those that have implemented the measures, one can not, however, expect a 100% performance, due to the size of the enterprises and the complexity of their enterprise networks, their IT use patterns, and the distribution of wireless communications. The same tendency as seen before appears here: large enterprises perform better on all measures compared to smaller.

The statistics on IT use show that 64% of the enterprises in the survey provide their employees with remote connection to the enterprise system, see Figure 4.1. The use of VPN to secure the communication is however much lower; 47%. This reveals that some enterprises have not secured their communication lines between enterprise systems and home office workers.

Except for VPN, the other measures are not comparable with foreign surveys. Compared with the 2005 FBI Computer Crime Survey [2], the Norwegian use of VPN matches the US level.

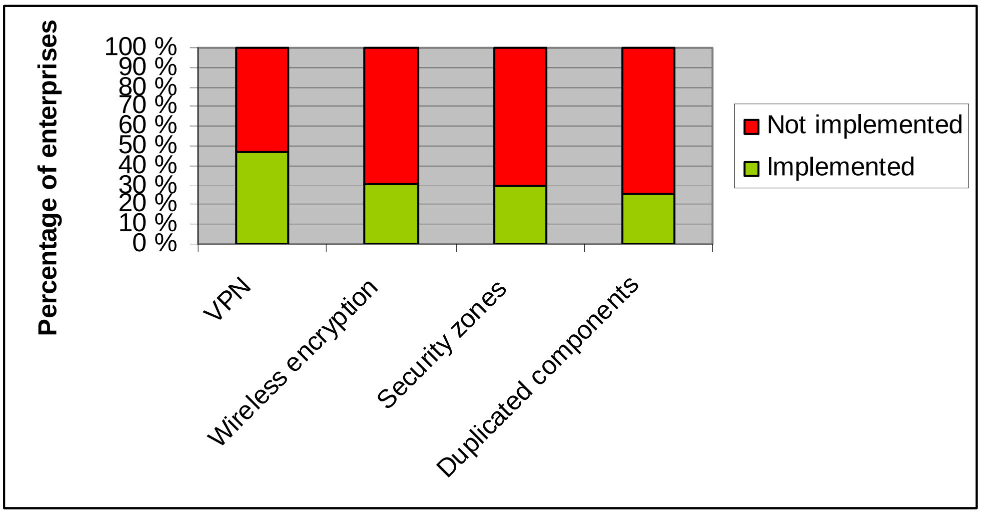

Figure 5.13 Security architecture, N=749

Moving on to traffic restricting measures, different filtering techniques become important. Firewalls and spam filter are widely applied, although large enterprises have implemented more of the measures compared to the smaller ones. Also foreign surveys [2] show a high degree of implementation of these technologies.

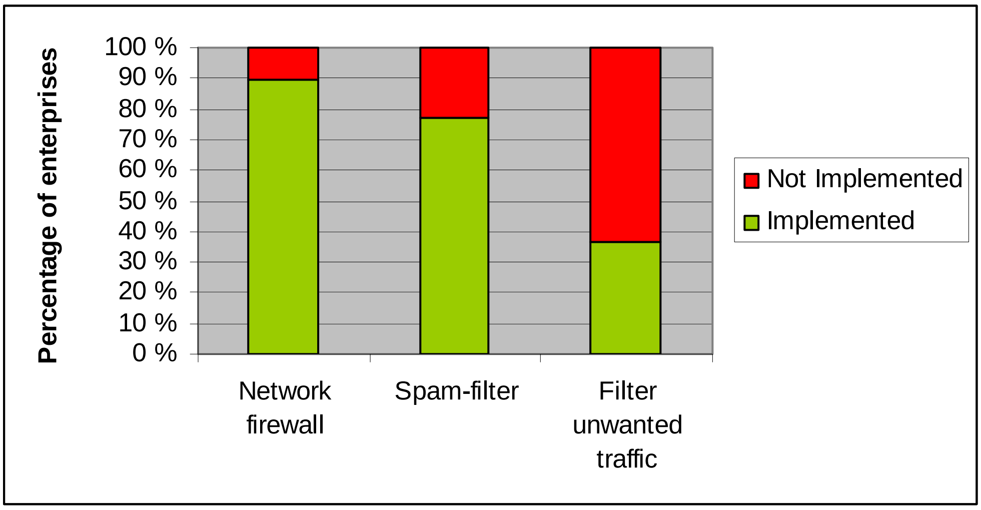

Figure 5.14 Traffic restricting measures, N=749

Patching security software and auditing the firewall are necessary steps to ensure that the security software delivers the required services. The 2006 survey addresses security routines among the enterprises, and the results document few known weaknesses in these critical routines. See Figure

5.15. It seems that the majority of the Norwegian enterprises at least occasionally update security software.

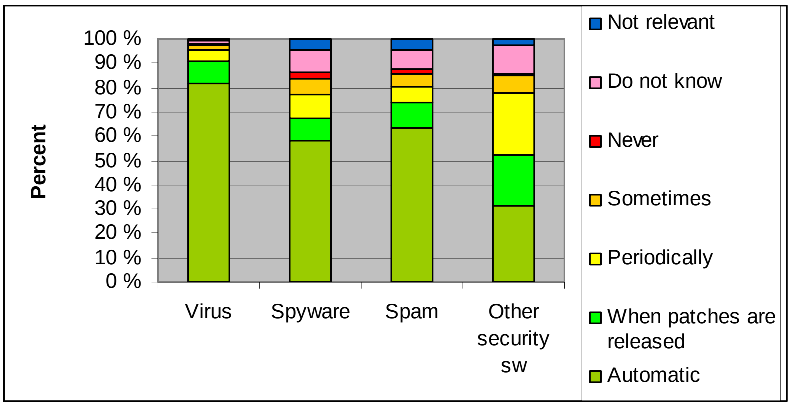

Figure 5.15 Updating frequencies of security software, 666<N<729[9]

Foreign surveys do not address similar updating procedure details; the UK survey [10] shows that 80% update their virus software daily.

When studying the frequency with which Norwegian enterprises review the firewall rules, we find that as much as 33% do not review these rules at all, see Figure 5.16. More than 50% of the enterprises with less than 25 employees never review the firewall rules, compared to 7% of the large enterprises with more than 500 employees.

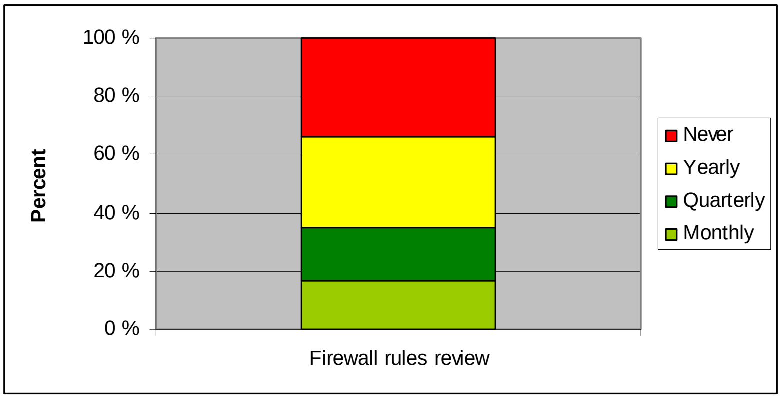

Figure 5.16 Firewall rules review, N= 684

Summary:

- Network security includes mainly preventive measures. Virus protection, network firewall and spam filter are the most commonly used technologies for protection against unauthorized traffic.
- It is uncommon to divide the network into security zones. Likewise, physical security measures, like duplication of critical components, are rare. These measures would have been useful in a defense in-depth strategy.

[9] Virus: N=792, spyware: N=678, spam filter: N=666, others: N= 689

- There is also room for improvements regarding securing communications between enterprise systems and remote users, and securing wireless access.

5.2 Security in outsourcing contracts

5.2.1 Good security principles in relation to outsourcing of IT operations

The word outsourcing reflects the use of external agents to perform one or more organizational activities. Outsourcing of information systems can be traced back to the 1963 agreement between Electronic Data Systems and Blue Cross of Pennsylvania for the handling of the latter's data processing services [15]. Since then, outsourcing has evolved and today includes a range of outsourcing models.

The literature reviews both strategic and economic reasons for outsourcing of IT operations. Outsourcing can for instance provide an organization with IT competence and resources that the organization does not have in-house [7]. Similarly, outsourcing can contribute to improved security if the organization does not have the specialized security expertise in-house. However, IT security is scarcely covered in literature on outsourcing. A library search on "risk in outsourcing" resulted mainly in research on economic risks exemplified by hidden costs, loyalty risks among own employees, risk to lose the rest of the critical in-house IT expertise, and the risk of developing a dependence on the outsourcing vendor [7][30].

The key issue in any outsourcing relation is the agreement of legally binding responsibilities and liabilities by the parties to the agreement [17]. The subcontractor will have access to the customer's data and to sensitive information. A customer should therefore ensure that a warranty is inserted into the contract ensuring that the provider complies with the security policy. If the outsourcing provider is suspected of security breaches, both parties should know the next step [10]. How security issues should be included in a service level agreement is discussed by [20]**.** The UK survey documents that 97% of the outsource providers follow the customer's security policy, while 7% have their own policy [10].

Outsourcing IT-services also requires very careful attention to security management. Both an organization and a process are needed to clarify responsibilities and liabilities. One of the most important processes is to enable customers to monitor and measure the compliance with the security requirements [17]. Without continuous measurements and reporting of the compliance with service level agreement, all else is nugatory [30]. The role of monitoring, to make sure that the services are delivered, will be performed by the internal IT staff [7]. So even if the enterprise outsources its IT resources, there needs to be a certain level of security competence in-house in order to specify the security policy and monitor the degree of compliance.

5.2.2 Outsourcing practices among Norwegian enterprises

Approximately 50% of the Norwegian enterprises in the survey outsource parts of or all their IT-operations. This corresponds with the results from the UK survey [10]. The answers from the 749 enterprises in the Norwegian Computer Crime Survey 2006 are illustrated in Figure 5.17.

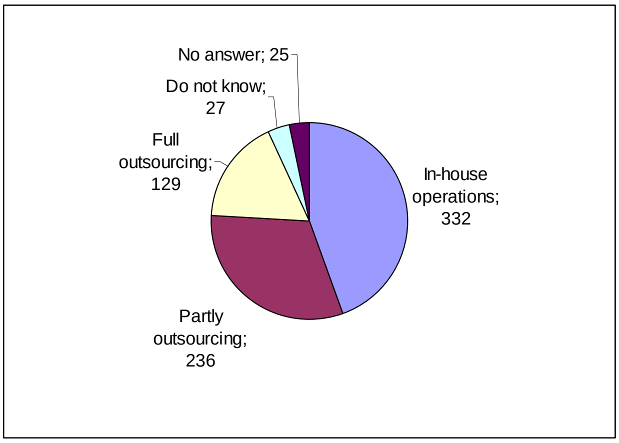

Figure 5.17 Degree of outsourcing, N=749

There are no surprising differences between various business segments. Enterprises in all branches, both in private and public sector, outsource their IT-operations, with only minor differences among them. There are no significant trends towards increased outsourcing among large or small enterprises.

Remarkably, we see that a small part of the enterprises do not know whether or not they outsource their IT operations. Among the smallest enterprises, as much as 18.4% are unaware of this. Among the enterprises with 6-10 employees, 17% do not know. Looking closer at the identity of the respondents, it appears that typically IT officers, financial managers or business managers answered the questionnaires. It should be expected that all these professions have sufficient insight into the outsourcing practices and contracts of their enterprise, yet, the results show otherwise.

About 11% of the 749 respondents define themselves as critical infrastructure enterprises. The data shows that among the enterprises that outsource all their IT operations, as much as 15.5% define themselves to belong to the group “critical infrastructure”. Similar numbers are 14.4% for those who partly outsource their IT operations and only 7.5% for those with in-house IT operations. This means that a slight majority of critical infrastructure enterprises outsource their IT operations.

A well-known strategy for modeling and analyzing information security is to apply defense-in-breadth and in depth. The survey covers breadth by including questions about both technological and organizational measures, and depth by incorporating the dimensions of prevention, emergency preparedness, detection and response. Even if an enterprise outsources parts or all of its IT operations, it still faces certain in-house security challenges on an individual level. To mitigate security challenges with own employees, security guidelines and education in information security could be suitable measures. Examining the security practices among the enterprises that do not oursource at all, those that partly outsource and those that outsource everything, we find no major differences in security practices regarding guidelines and education of end-users. Among those who keep their IT operations in-house, 66% have user guidelines, which equal the number for those who have outsourced all their IT operations. The corresponding number for those who partly outsource is 70%. Looking at the education of own employees, we find that 42% of those who keep their IT-operations in-house provide some kind of education in IT security, equal to those that partly outsource their IT-operations. 38% of those outsourcing all their IT operations provide some kind of education of employees.

Summary:

- All kind of enterprises outsource IT operations; there is no clear tendency.
- There are no major differences in the implementation of user guidelines and education of own employees between enterprises that keep their IT operations in-house and those that outsource parts or all of their IT operations.
- The critical infrastructure enterprises outsource IT operations more frequently than other enterprises.

5.2.3 Security and liability requirements in outsourcing contracts

Access control to enterprise sensitive data is a fundamental security service. Ideally, one could argue that all enterprises should have such a requirement included in the contract. The analysis shows that 67% of those that have outsourced all their IT operations have similar requirements included. The equivalent number for those that have partly outsourced their IT-operations is 56%, see Figure 5.18. The UK survey [10] reveals that among UK companies, a large majority of outsourcing providers follow their customers' security policy.

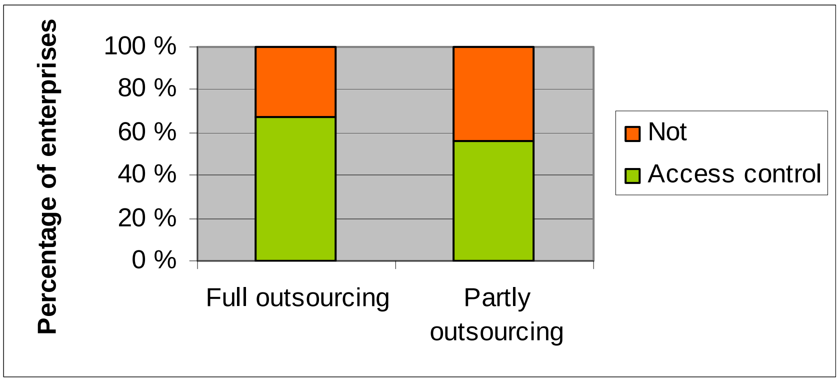

Figure 5.18 Access control requirements in outsourcing contracts, N=380

Requirements regarding security technologies and routines could also be included in outsourcing contracts. Examples of technologies and routines are firewalls, intrusion detection technologies, and routines for updating operating systems and security software. Such technologies and routines can preserve confidentiality and integrity of the enterprise information. The survey results show that 71% of those that have outsourced all their IT operations do include such requirements in their outsourcing contracts. The equivalent number for those partly outsourcing is 56%, see Figure 5.19.

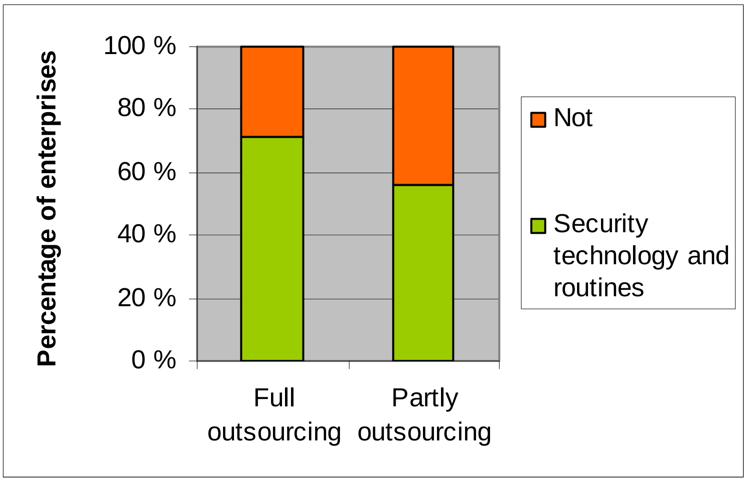

Figure 5.19 Requirements in outsourcing contracts regarding additional security technologies, N=380

Regarding the definition of information security, availability is often seen as "the third leg", which must be in place in addition to confidentiality and integrity. The survey results indicate a small increase in awareness regarding this issue. 71% of those that have outsourced all IT-operations and 61 % of those that have outsourced parts of their IT operations have included availability of system or services in the contract requirements, see Figure 5.20.

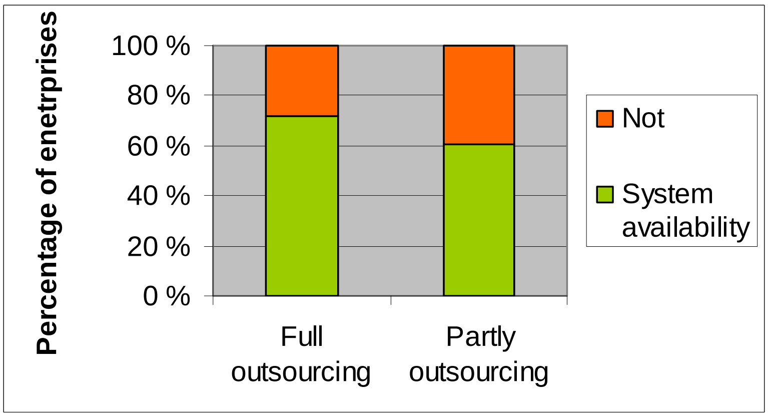

Figure 5.20 Availability requirements in outsourcing contracts, N=377

Step number two in the defense in-depth strategy is audit, which provides a capability to detect incompliance with security requirements. A study of the answers regarding inspection of security routines reveals that 53% of those that have outsourced all IT operations have requirements regarding inspection. The corresponding number for those who partly outsource is 41%, Figure 5.21.

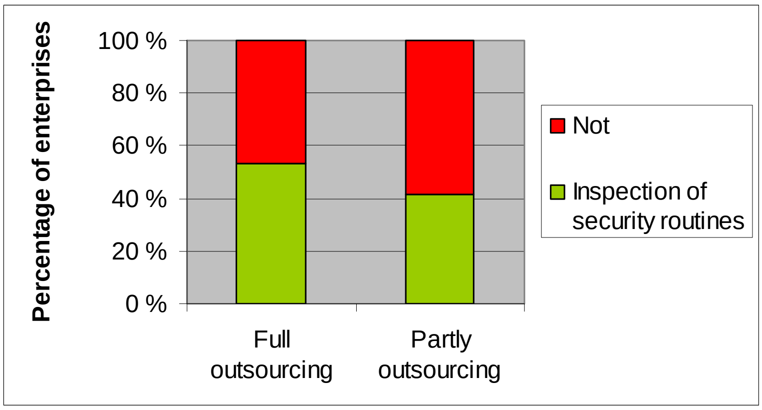

Figure 5.21 Inspection of security routines, N=373

The lack of requirements in the contracts becomes even more obvious when we look at the practice of evaluating or measuring the security level, see Figure 5.22. Only 36% of the enterprises that outsource all their IT operations have such a requirement included in their contracts. This drops to 25% among those who partly outsource their IT operations. Compared with how well the enterprises specify the initial requirements, we observe a clear decline in the focus on detection capability regarding compliance to security routines. One hypothesis explaining these findings is that there is a strong and trusted relationship between vendor and customer.

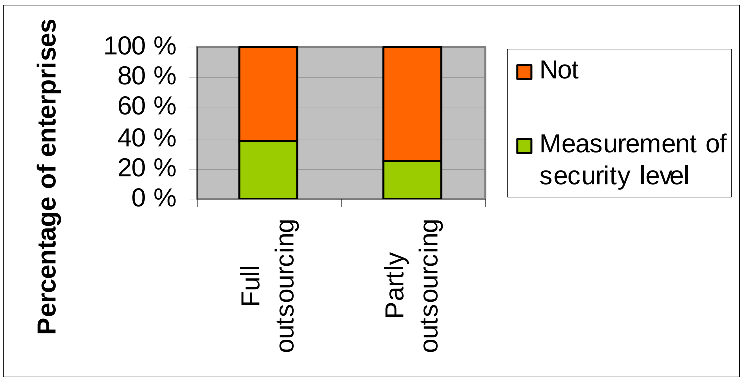

Figure 5.22 Rights to measure the security level in outsourcing contract, N=371

As we move further into the defense in-depth strategy, it becomes apparent that the requirements in the outsourcing contract increasingly do not cover the last line of defense. If the outsourcing partner does not fulfill his obligations or misuse the client’s systems in some way, this should have consequences. Looking to the survey results, we notice that a minor share of the enterprises that outsource parts or all of their IT operations have requirements with respect to liability for compensation included in the contracts. Among those that have outsourced all their IT-operations, as few as 25% have included economic penalties in the contracts. The corresponding figure for those that partly outsource is even lower, 20%, see Figure 5.23.

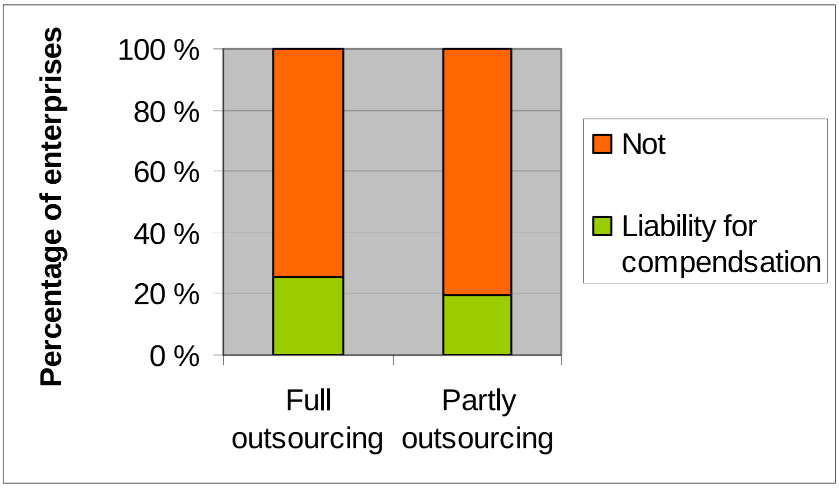

Figure 5.23 Liability for compensation, N=370

Studying other sanctions, see Figure 5.24, the picture is slightly better, although there are large holes. 24% of those that outsource all their IT operations have some kind of sanctions included in the contract, compared with 26% of those which partly outsource their IT operations.

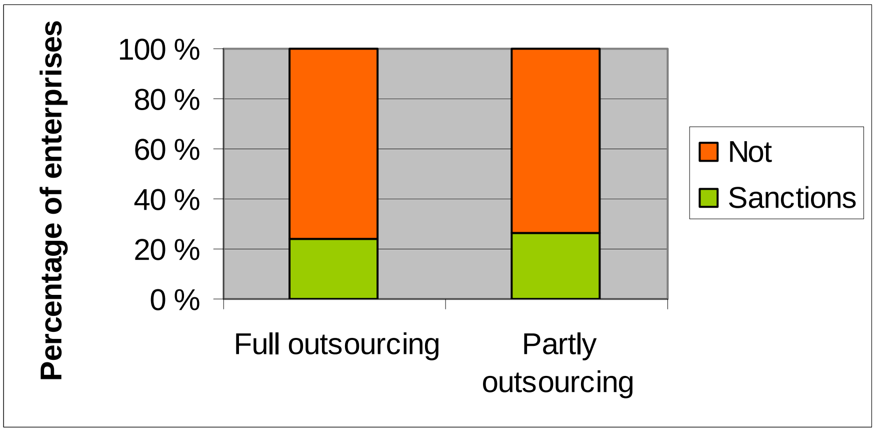

Figure 5.24 Sanctions in outsourcing contracts, N=369

Summary:

- There are indeed large holes in outsourcing contracts regarding the regulation of information security, and the holes expand when moving down the defense-in-depth line.
- Most attention is given to securing the availability of the outsourced systems and least attention to liability for compensation if the vendor does not comply with the requirements.

6 Do enterprises that implement many security measures report fewer incidents, less losses, or higher financial returns than those that do not?

6.1 Correlations between security level and security incidents

The NCCS06 asks questions about risk (number of incidents and economic losses) and registers economic performance (return of investment). When enterprises invest in security, we assume that this is done because of expected returns of the investments. We wanted to study if the data showed any patterns that confirmed relationships between security investment and returns, like risk reduction or improved economic returns. We applied factor analysis with varimax rotation to reduce the number of variables and simplify the analysis. The factor analysis revealed 5 factors from a total of 25 security measures (6 organizational security measures and 19 technical security measures). Then, the factors were reliability tested. Crobach's alfa values above 0.7 are good. Table 6.1 shows the results of the reliability tests of the factors. Three factors were single measures. These three factors are vulnerable because they depend on only one question.

Table 6.1 Factors derived from factor analysis and used in subsequent analysis

Indexes	**Security measures included in the index**	**Cronbach's alfa**
Holistic security	Locked server room (H1)	0.742
	Filter against unwanted traffic (H2)	
	Plans to handle security breaches (H3)	
	Duplication of critical components (H4)	
	Backup power supply (H5)	
Computer security	Anti virus software (C1)	0.715
	Network firewall (C2)	
	Spam filter (C3)	
	Backup(C4)	
Biometrics	Biometric authentication	0.636
Passwords	One time passwords	0.729
Human focus	End user education	0.616

Two indexes were derived with values between 1 and 0. They were named "Holistic Security Index" and "Computer Security Index", after the kind of security measures included in the indexes.

Holistic Security Index= (H1+H2+H3+H4+H5)/5

Computer Security Index= (C1+C2+C3+C4)/4

Spearman correlation analysis was applied on the indexes as shown in Table 6.1 and the number of incidents reported in the survey. The correlation coefficients vary between "0" and "1". A correlation coefficient of "0" means that there is no correlations at all between the ranks of the tested variables. A correlation coefficient of 1 means perfect correlation between the ranks of the tested variables.

Table 6.2 Correlations between security measures and computer crime incidents at 5% level (non-significant correlations are not shown)

	Incident	**Holistic security**	**Computer security**	**Biometrics**	**Passwords**	**User education**	**Responses (N)**
Vulnerabilities of employees	Misuse/abuse of IT resources	0.244	0.104		0.106		481
	Extortion attempts						526
Vulnerabilities in architecture	DoS attack	0.090	0.112				484
Vulnerabilities in software	Hacking	0.170	0.094	0.088			519
	Unauthorized copying of data						493
	Unauthorized altering of data	0.101					503
	Illegal distribution of data						486
	Internet fraud by using credit cards	0.086		0.172			536
	Virus/worms Trojans	0.095					521
Vulnerabilities in physical security	Theft of IT equipment	0.301	0.158		0.132	-0.085	575
	All incidents	0.314	0.205	0.079	0.077		736

Table 6.2 shows that we in many cases can reject the hypothesis (H_0) that there are no correlations between the total number of security incidents and the security measures implemented. The results document, however, that Holistic Security Index correlates positively with 7 incidents, although the correlation coefficients are weak. Then, Computer Security Index correlates with 4 incidents. The result also shows that the strongest correlation coefficients are achieved when the dependent variable is the count of all incidents.

Which enterprises achieve full score on the holistic security index? By sorting the data we find that there are 68 enterprises that have implemented all security measures and get a maximum score on Holistic Security Index. Studying the data in more detail, we see that the 68 enterprises consist of significantly many public and large enterprises when compared with the total reduced sample of 736 enterprises[10]. Also looking at which industries they belong to, we see that a remarkably high number of these 68 enterprises are from industries like oil/gas, industry, electric power supply, IT/telecommunication, transportation, banking/finance and health/social services. They represent typical critical infrastructures. This is confirmed by the respondents: 73,5% of the 68 enterprises define themselves as critical infrastructure enterprises in contrast to only 10.6% of the total sample of 736 enterprises. Furthermore, the data analysis shows a significant correlation (0.485) between Holistic Security Index and Computer Security Index. (505 enterprises have implemented all the computer security measures.)

Applying a new dependent variable – the average reported incidents per employee – we can repeat the correlation analysis procedure. We study the results when compensating for the scale factor: the number of employees. Table 6.3 shows the new results.

We observe that there are just minor reductions in the number of correlations and absolute values of the correlation coefficients, thus we still reject the hypothesis that there are no correlation between security measures and reported incidents. Therefore, it is reasonable to think that a wide range of implemented security measures contributes to improved detection ability.

[10] The data set is reduced as outliers are removed, see chapter 3.4.

Table 6.3 Correlations between security measures and the average number of incidents per employee (insignificant correlations at 5% level are not shown)

	Incident	**Holistic security**	**Computer security**	**Biometrics**	**Passwords**	**User education**	**Responses (N)**
Vulnerabilities of employees	Misuse/abuse of IT resources	0.239	0.100		0.099		481
	Extortion attempts						526
Vulnerabilities in architecture	DoS attack						484
Vulnerabilities in software	Hacking	0.168	0.094	0.087			519
	Unauthorized copying of data						493
	Unauthorized altering of data	0.097					503
	Illegal distribution of data						486
	Internet fraud by using credit cards	0.086		0.171			536
	Virus/worms Trojans						520
Vulnerabilities in physical security	Theft of IT equipment	0.244	0.123	0.096		-0.092	574
	Incidents per employee	0.184	0.136				736

An attempt to perform a linear regression analysis of the indexes as independent variables and the reported incidents as dependent variable provided no further information. The explanation power of the model measured as R^2 was very low (below 5%).

Summary:

- There are several significant positive correlations between security measures and the reporting of computer crime incidents; this means that those with implemented security measures also report more incidents compared with those with fewer measures implemented.

- A holistic security regime, which is typically implemented by critical infrastructure enterprises, correlates positively with half of the incident categories reported in the survey.
- The strongest correlations are seen between holistic security regime and theft of IT equipment and misuse/abuse of IT-resources.
- Computer security measures correlate positively with reporting of incidents, though with fewer incidents compared to the holistic security index.
- The correlation coefficients are weak, yet significant (low absolute values on the correlation coefficients). This may indicate a cause-effect relationship: enterprises with more security measures implemented have a better ability to detect computer crime incidents.

6.2 Correlations between economic performance and security incidents

It is also interesting to study if there are any correlations between typical economic performance indicators, such as return of investment and reported economic losses due to computer crime.

Table 6.4 Correlations between security measures and return of investment before tax (insignificant correlations at 5% level is not shown)

	Holistic security	**Computer security**	**Biometrics**	**Passwords**	**User education**	**Responses (N)**
Reported economic losses because of computer crime	0.223	0.188				201
Return of investment	0.325	0.163		0.124		719

The hypotheses (H_0) are tested: *There are no correlations between security investments and return of investment before tax.* Table 6.4 shows that a holistic security and computer security regime correlate with higher economic performance measured as return of investment and reported economic losses because of computer crime.

We introduce a new indicator by calculating the average return of investment per employee as dependent variable; then we can adjust the variable for economies of scales effect. Now, Spearman correlation analysis shows only one significant correlation between a holistic security regime and return of investment per employee. Although the statistical software came out with a significant correlation, the low absolute value of the correlation coefficient, 0.075, indicates a weak relationship. Thus, we reject the hypothesis (H_0) that there are no significant correlations between security investments and return of investment before tax. One possible explanation is that security measures contribute, but only to a low degree, to return of investment. We van not reject H_0 above.

We also wanted to test the 0 hypothesis (H_0): *There is no correlation between security investments and reported losses.*

Only 88 enterprises out of 202 answered the question about economic losses. Only 1 out of 10 of the respondents has routines to calculate the economic losses. The numbers of reported losses might therefore have low validity. Aware of this potential weakness, we applied Spearman correlation analysis to the data to study correlations between the total reported losses and the security investments. Spearman correlation analysis reveals only two significant correlations at 5% level:

– Holistic security and total reported losses:	0.233
– Computer Security and total reported losses:	0.188

Consequently, those enterprises that have invested in security also report larger total losses. This makes sense because we know that those enterprises with most implemented security measures are dominated by large critical infrastructure enterprises. Large enterprises have large revenues and a corresponding high potential of losses.

If we calculate the correlation coefficients between the factors “Holistic Security”, “Computer Security”, and the average loss per employee, there are no significant correlations. Our interpretation is that there is no evidence that investing in security measures contribute to reduced loss per employee. However, emphasis should be put on the low validity of the reported economic losses, which means that we can neither claim that security investments do not have an impact on the losses.

Then, linear regression models with the indexes as independent variables and the economic performance indicators as dependent variable, was produced. The explanation power R^2 was however extremely low, and the model did not provide further information.

Summary:

- Analysis of this data set indicates that security investments correlate significantly and positively with return of investment. However, the absolute value of the correlation coefficient is low, meaning that the relationship is weak. We found no significant correlation between security investments and the average reported losses per employee. One possible explanation of these findings is that other management input factors explain the majority of the economic return variance, leaving security to have a minor role. It must also be emphasized that low validity of the reported economic losses makes the results uncertain.
- Large critical infrastructure enterprises make more money and report higher losses. They have also put more emphasis on security measures.

7 SWOT analysis of the Norwegian Computer Crime Survey

The SWOT Analysis is used to evaluate the Strength (S), Weaknesses (W), Opportunities (O) and Threats (T) involved in a product. The internal factors are described by the strengths and weaknesses, while the external or environmental factors are presented by the opportunities and threats. A clear objective should be defined before a SWOT analysis is conducted. The SWOT analysis helps to pursue the objective. We have suggested the following objective for the Norwegian Computer Crime Survey:

The Norwegian Computer Crime Survey should be a frequent event which maps and analyses the security status and the number of computer crime incidents in Norwegian businesses. If same questions are addressed over time, the time series data could serve as an information security barometer[11].

An Information Security Barometer could provide the government with a measurement tool for enterprises compliance with good security practices. The barometer can be used to follow up the national ambitions of information security.

The rationale behind this objective is the lack of national statistics on computer crime and security practices. Business values consist of information and knowledge, and some of the information is sensitive and require protection. As new information technology is developed and applied by enterprises, new risks will be introduced. The government has developed strategies for information security [16], but has few possibilities to obtain information about the security status of those businesses that are not frequently under supervision of a national authority. Moreover, different laws, regulations and supervision methodologies impede the making of comparisons between different sectors. We believe that the ideas of security metrics for management [5][6][26] can be utilized also on a national level, to produce a measurement tool for information security and to reveal trends. The NCCS represents an opportunity for future security measurements.

The SWOT analysis framework is shown in Table 7.1.

[11] DSB has developed a security barometer for society vulnerability.

Table 7.1 SWOT analysis of the Norwegian Computer Crime Survey 2006

	Internal factors		**External factors**	
	Strengths	*Weaknesses*	*Opportunities*	*Threats*
The survey quality				
The working committee quality				

The quality of the survey and the working committee of the survey are discussed according to the SWOT scheme. The quality of the survey relies on its relevance according to the proposed goal, the validity and the reliability, and the potential for subsequent statistical analysis. The working committee quality constitutes expertise, which the members brought in and the organization of the work. According to the SWOT scheme, the quality of the survey can be characterized according to the following aspects:

<u>Internal factors:</u>

- The survey provides information on a wide range of security measures and computer crime threats. *(Strength)*
- It encourages the respondents to answer honestly by providing anonymity.*(Strength)*
- Binary questions about which security measures the enterprises have implemented are easy to answer and provide robust answers. *(Strength)*
- The questionnaire contains several ambiguous questions, for instance about VPN, exercises, education. *(Weakness)*
- Some questions are not well-suited to evaluate the security status, for instance questions about the use of personal passwords. It would have been better to address the strength of the applied passwords since personal passwords are widely used and are important security measures. *(Weakness)*
- Binary questions provide little information and are difficult to analyze by more advanced statistical techniques. Scale variables could provide more information and be more useful regarding further analysis and research. *(Weakness)*
- Applying a holistic security view, some questions are missing on reactive measures, for instance on forensic tools and evaluation/learning processes after the incident. *(Weakness)*
- There is no established systematic analytical framework to interpret the findings from year to year, and to study trends. *(Weakness)*
- There are missing links between reported computer crime incidents and their consequences because the consequences are reported without relation to each computer crime incident. *(Weakness)*
- The numbers of incidents and the economic losses reported in the survey are doubtful. Computer crime incidents are difficult to detect, and many enterprises do not have

systems or routines that help detecting incidents. A minority have routines for calculating losses due to computer crime incidents. Some guidelines for calculating losses should be included. *(Weakness)*

External factors:

- More knowledge on information security and higher general security awareness may improve the information security awareness and the validity of the numbers of reported incidents and economic losses. *(Opportunity)*
- More visualized support from supervisory authorities may strengthen the reputation of the survey, thus increasing the response rate and making it more useful for research and student work. *(Opportunity)*
- Better resources enable the use of more expensive, but better, interview techniques (telephone interviews) and delivers a higher response rate. *(Opportunity)*
- Many competing surveys make the respondents reluctant to participate in surveys in general. *(Threat)*
- Higher security awareness makes the respondents more reluctant to answer questions on the information security policy and practices. *(Threat)*

According to the SWOT scheme, the working committee can be characterized by the following aspects:

Internal factors:

- The computer crime committee at NSR consisted of persons with good knowledge about information security practices and computer crime. *(Strength)*
- An experienced social science statistical expert was not engaged because of lack of resources. It had impact on the design of the survey, the type of questions addressed in the survey and subsequent analysis. *(Weakness)*

External factors:

- If the financial situation improves, an experienced social science statistician could be engaged in the work from the design phase and throughout the analysis. *(Opportunity)*
- Participating in these meetings was voluntary, which made it difficult for committee members to give high enough priority to the work. *(Threat)*

Summary: Up to now, the surveys have shed light on the high dark computer crime numbers, and then documented weaknesses in security regimes. The reported computer crime numbers and economic losses are however doubtful due to low validity. The validity of reported economic losses is low because the enterprises lack routines on reporting incidents and estimating the losses. These numbers are best guesses. The validity of reporting losses can be improved by more detailed instructions on how to measure, for instance, losses. The validity of the computer crime numbers is more challenging to improve, due to the characteristics of computer crime incidents. Many of them are not easily detected. Besides, remembering the exact number of crime incidents for one calendar year is an impossible task if the enterprises do not register the incidents continuously. This also impacts the reliability. Studying the answers, we see that many of the reported incidents are rounded numbers and best guesses. The survey produces a rough estimate on the dark numbers.

Potential follow up strategies can be outlined from the SWOT analysis by answering the following questions:

- How can we use the strengths?
- How can we avoid the weaknesses?
- How can we exploit the opportunities?
- How can we defend against the threats?

One strategy is to exploit the strengths and opportunities by reinforcing the links to the national security work and scientific research on information security. Increased cooperation with relevant authorities and research institutions could improve the quality of the survey. Improved quality could also make the survey more relevant to enterprises and consultants, and hence strengthen the utility of the results and the willingness to put money into the survey.

Another and complementary strategy is to reduce the weaknesses and fight the threats by improving the questionnaire, its design and the analysis process. This is necessary to strengthen the trust of the survey and the quality of the data.

Then, why should one spend money on such surveys, measuring the security status, when the result, as documented in this report, shows that security measures do not reduce the number of incidents and the economic losses, and just slightly improve the return of investment? First, the validity of the dependent variables, like number of computer crime incidents and reported losses, are probably low. Therefore, they do not provide correct information. Second, it is also reasonable to believe that other management input factors than security has larger impact on economic returns. Third, it is important to detect incidents, and by analyzing the data we find that security measures correlate with detection ability (reported incidents). Those enterprises that have implemented security measures more often report incidents compared with enterprises lacking security measures. To improve the detection ability, it is therefore important to stimulate enterprises to implement security measures. Referring to research within the safety field [38] and the effectiveness of safety measures, we know that most of the economic variance can be explained through management factors in general. This might well be the case here, but as we have not collected data on general management variables, we are not able to conduct analysis to confirm or reject the statement.

8 Conclusion

The aim of this report has been to document the work with the design of the questionnaire for the Norwegian Computer Crime survey 2006, to present the results within a measurement framework for good security principles, and to study the relationships between security measures and performance, measured as security incidents and financial returns and losses. The theoretical foundation has been best practices and security metrics for management. In addition, a simple SWOT analysis has been performed to discuss and suggest further improvements for the survey.

How vulnerable are Norwegian Enterprises for outages in Internet services and how serious are the consequences of the reported computer crime incidents?

The data analysis confirms that Norwegian enterprises strongly depend on IT and the Internet. The results also show an increase in the number of respondents reporting that critical consequences occur after short-term system disruption compared with the 2003 survey. Even if the respondents claim that large consequences will occur if the systems are down, this does not correspond with the reported consequences of those victim of computer crime incidents. In general, it seems that the respondents judge the real consequences to be small or not notable. This result is in line with the marginal reporting of incidents to the police. In addition, the results show that few enterprises seek external assistance after being hit by incidents. Besides, the costs are reported to be low, also compared with foreign surveys, but it should be remarked that very few have routines in place for calculating the losses of computer crime incidents, and that the validity of in particular these answers is low.

Which security measures have Norwegian enterprises implemented to mitigate computer crime and how does this practice correspond with good security principles?

The survey addresses a number of security measures, and two important tendencies should be noted. First, it is a trend that large enterprises have implemented more security measures than smaller enterprises. Large enterprises more often have dedicated positions responsible for information security. This is not surprising due to the increased complexity of IT systems in large organizations. Large organizations also possess more resources. Another obvious pattern is that the use of mature preventive measures is more widespread, compared to measures that intend to detect and react if incidents occur. We also see the same tendency in outsourcing security: liability and sanction are rarely included in the outsourcing contracts, in contrast to preventive measures. This makes the buyers vulnerable to potential failures and weaknesses of the outsourcing partner. These findings can also be connected with the low percentage of enterprises which have routines for calculating the economic losses of computer crime. Compensation for losses is not emphasized. A few organizational measures are examined in the survey, and these are used to a lesser extent compared to many preventive security technologies. User education and exercises are, in particular, implemented by few enterprises. Compared with good security principles, the results reveal holes in the security strategies, particularly behind the perimeter security. Also organizational security measures have inherent weaknesses as few enterprises train or educate their employees in information security.

Do enterprises that have implemented many security measures report fewer incidents and less losses, or higher financial returns, compared with those that have invested less in security measures?

The answer to the first part of the question is clearly “no”. Spearman Correlation Analysis shows that those that have implemented more security measures more often report some kinds of security incidents when compared with those that do not. This may indicate that not all computer crime incidents are reported in this survey, because enterprises with low detection abilities do not see all the incidents. The reported incidents do not provide exact information but are rough estimates. A metaphor for computer crime incidents is an iceberg. A few incidents are reported to the police, more are detected and reported in surveys, but there are still a lot of incidents that are “below the waterline” and not seen at all. Studying the relations between implementation of security measures and the reporting of incidents in more detail, we find significant correlations between security measures and incidents: typically, a holistic security regime correlate with reporting of several types of incidents.

The results reveal also a significant relationship between security measure investment and return of investment. The correlation coefficient is weak, however, indicating that security measures have a small contribution to the return of investment. Studying the data in more detail, it seems apparent that large and critical infrastructure enterprises report higher return of investment, but also higher losses due to computer crime incidents. They also have more security measures implemented. But, when we study the economic return of investment per employee, we find just one weak correlation between Holistic Security Index and return of investment before tax, and no correlations between security investment/measures in general and reported economic losses. We can reject the 0 hypothesis (H_0) that there are no correlations between return of investment and security investments, but the weak correlation coefficient indicates that good economic performance may result from other than security factors, for instance the industry they belong to, economics of scale, or management factors in general. This explanation corresponds with the experience gained by evaluating the effects of safety investments. We have not been able to find documentation that describes the safety measures or how they contribute to economic results. However, one can agree that they are important for other reasons. The correlation analysis of reported economic losses and security measures reveals no significant correlations. A possible explanation is low validity of the answers.

What are the strengths and weaknesses of the Norwegian Computer Crime Survey 2006 questionnaire and process, and how could the survey become a security measurement tool for the government?

Since Norwegian authorities lack good and complete statistics on computer crime, the survey is a useful tool for measuring the security level and the threats against IT systems. Therefore, the survey has a potential as a security barometer on a national level. It also has the potential to serve as a benchmarking tool for enterprises if the survey and the questions are further improved, more data is collected, and indexes are developed for different industries and enterprise sizes. This will require a standardized analytical framework, more unambiguous questions, and also a predictable financial situation for future surveys. Cooperation with research institutes can improve the tool, the quality and the analysis of the questions, and the use of the collected data.

9 The way ahead

This report draws the big picture of information security and computer crime in Norwegian enterprises. Previous research and surveys on computer security have focused on security technologies. We know more about the use of security technologies and the effectiveness of security technologies than organizational security measures. The 2006 survey examines for the first time organizational security measures and awareness raising initiatives in the population of Norwegian enterprises. The results indicate that many organizational measures, in particular those aiming to change human minds, are to a low degree implemented in the organizations. Studying the taxonomies, it seems that the organizational measures are also important in a defense-in-depth strategy, in which Norwegian enterprises perform less well. Further studies on organizational security measures and their effectiveness will be an important area for future research. The following research questions are relevant and will be addressed in subsequent studies:

- Which organizational security measures do enterprises use?
- How do information security managers regard the effectiveness of organizational security measures?

More specific:

- How do security policy and guidelines change behavior and raise security awareness in organizations?
- What is the effect of educating employees; is it worth the effort?

References

[1] Johansson, E, Johnsson, P., Assessment of Enterprise Information Security – the Importance of Prioritazion, *Proceedings of the 2005 Ninth International EDOC Enterprise Computing Conference (EDOC'05)*, 2005.

[2] Federal Bureau of Investigation, 2005 *FBI Computer Crime Survey*, January 2006.

[3] Næringslivets sikkerhetsråd (NSR), Senter for informasjonssikring (SIS) and ØKOKRIM., *Mørketallsundersøkelsen 2003 – om datakriminalitet og IT-sikkerhet*, (In Norwegian), English title: Norwegian Computer Crime and Security Survey 2003, 2004.

[4] Cashell, B, Jackson W.D., Jickling, M., and Webel, B., *The Economic Impact of Cyber Attacks*, Congressional Research Service Report, 4/1/2004, p 1-45.

[5] Kovachich, G., Information Systems Security Metrics Managements, *Computers and Security*, 16 (1997), pp 610-618.

[6] Kovacich, G. L., Halibozek, Edward P., *Security Metrics Management. How to Manage the Cost of an Asset Protection Program*, Elsevier Inc, New York, 2006, pp 1-319

[7] Martinson, M. G., Outsourcing Information Systems: A Strategic Partnership with Risks, *Long Range Planning*, Vol. 26, No 3, 1993, pp 18-25.

[8] Kotulic, A. G, and Clark, J. G., Why there aren't more information security research studies", *Information & Management*, Volume 41, issue 5, May 2004, pages 597-607.

[9] Gordon, L A., Loeb, M P., Lucyshyn, W and Richardson, R., *2006 CSI/FBI Computer Crime and Security Survey*, July 2006.

[10] Price Waterhouse Coopers, *DTI Information Security Breaches Survey*. Technical report, April 2006.

[11] AUSCERT, "2006 Computer Crime & Security Survey".

[12] Post & Telestyrelsen, *Mörkertalsundersøkningen 2005, Svenska organisationer om IT-säkerhetsincidenter*, (In Swedish). 5. July, 2005.

[13] Næringslivets sikkerhetsråd, *Mørketallsundersøkelsen om datakriminalitet 2006*, (In Norwegian), September 2006, pp 1-16.

[14] GAO, United States General Accounting Office, Washington DC 20548. *Information Security: Technologies to Secure Federal Systems*. GAO-04-467 Information Security, 85 pp.

[15] Dibbern, J., Goles, T., Hirscheim, R. and Jayatilaka, B., Information Systems Outsourcing: A Survey and Analysis of the Literature, *The DATA BASE for Advances in Information Systems* – Fall 2004, Vol 35, No.4, pp 7-102.

[16] Fenn, C., Shooter, R., and Allan, K., IT Security Outsourcing, How safe is your IT Security, *Computer Law & Security Report*, Volume 18, Issue 2, 31 March 2002, pp 109-111.

[17] Sherwood J., Managing Security for Outsourcing Contracts, *Computers & Security*, (16) 1997, pp 603-609.

[18] Ministry of Defence, Ministry of Trade and Commerce and Ministry of Justice and the Police, *National Strategy for Information security: Challenges, Priorities and Measures*, June, 2003.

[19] Næringslivets sikkerhetsorganisasjon (NSO) og ØKOKRIM. (In Norwegian), *Mørketallsundersøkelsen 2001*, English title: Norwegian Computer Crime and Security Survey 2001, 2001.

[20] Ronda R H., Security service level agreements: quantifiable security for the enterprise?, *New Security Paradigms Workshop Archive.* Proceedings of the 1999 Workshop on New Security Paradigms Table of Contents. Caledon Hills, Ontario, Canada, Pages: 54 - 60.

[21] Boni C. W., Kovachich G. L., *I-Way robbery. Crime on the Internet*, Butterworth Heinemann, Boston, 1999, pp 1-231.

[22] Wessels, M., *Computer, self and society*, Prentice Hall, New Jersey, 1990, 1-274.

[23] The Minstry of Justice and the Police, *NOU 2007:7 Lovtiltak mot datakriminalitet. Delutredning II. Utredning fra Datakrimutvalget oppnevnt ved kongelig resolusjon 11.januar 2002.* Avgitt til Justis- og politidepartementet 12.februar 2007".

[24] Schneier, B., *Secrets and lies. Digital Security in a Networked World. With new information about post 9/11 security*, Wiley Publishing, Inc, 2004, Second edition, pp 1-414.

[25] Stoll, C., *The cocko's egg. Tracking a Spy Through the Maze of Computer Espionage*, Pocket books, New York, 1990, 402 pages.

[26] Swanson, M, Barthol, N, Sabato, J, Hash, J and Graffo, L., *Computer Security. Security Metrics Guide for Information Technology Systems*, NIST Special publication 800-55, July 2003, pp 1-99.

[27] Vaughn, R.B., Henning, R., Siraj, A., Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, *Proceedings of the 36th Hawai International Conference on Systems Sciences*, 2002, IEEE.

[28] Ward, P. and Smith C., The Development of Access Control Policies for Information Technology Systems, *Computer & Security*, Volume 21, Issue 4, 1 August 2002, 365-371.

[29] Andersson, L. S., *Datakriminalitet i Norge. De mørke tallene*. Master Thesis. Gjøvik University College, 2007.

[30] Pemble, M., Transferring businesses and support functions: the information security risks of outsourcing and offshoring (A beginner's guide to avoid the aborgation of responsibility), *Computer Fraud & Security*, Volume 2004, Issue 12, December 2004, pp 5-9.

[31] Statistics Norway (SSB)., Nøkkeltall om informasjonssamfunnet 2006, pp 70-91. http://www.ssb.no/emner/10/03/sa_ikt/sa89/sa89.pdf Downloaded 2007.10.01

[32] Vivien K. G. L., Thompson S. H., Theo, G. L. L., Cyberloafing in an Asian Context. How do I loaf here? Let me count the ways, *Communications of the ACM,* January 2002, Volume 45, No 1.

[33] Keeney, M, J.D, Kowalski, E, Cappelli, D, Moore, A, Shimeall, T, Rogers, S., *Insider Threat Survey. Computer System Sabotage in Critical Infrastructure Sectors,* Carnegie Mellon Software Engineering Institute, U.S Secret Service and Cert Coordination Center, May 2005, pp1-45.

[34] Zhang, D., Oh, L-B, Theo, H-H, An Experimental Study of the Factors Influencing Non-Work Related Use of IT Resources at Work Place, *Proceedings of the 39th Hawaii International Conference on System Science*, 2006.

[35] Malcon, A., *Social Engineering. A means to violate a computer system (updated June 2006)*, Sans Institute 2007, 12 pp.

[36] Doherty, N.F. and Fulford, H., Aligning the information security policy with the strategic information systems plan, *Computers & Security*, Vol 25 No 1, 2006 pp. 55-63.

[37] Symantic, *Symantic Internet Security Threat Report. Trends for January-June 07*, Vol Xii, Published September 2007.

[38] Simonds, R.H. & Shafai-Sahrai, Y.: Factors Apparantly Affecting Injury Frequency in Eleven Matched Pair of Companies, *Journal of Safety Research*, 1977, 9, 120-127.