NTNU
Innovation and Creativity

Value of Investing in Information Security

A metastudy initiated by norSIS

Marie Kristin Johansen

Master of Science in Communication Technology
Submission date: May 2007
Supervisor: Jan Arild Audestad, ITEM

Norwegian University of Science and Technology
Department of Telematics

Problem Description

Is it beneficial for small companies to invest in good information security? The thesis should attempt to provide estimates on risk of loss, efforts in market and cost of security.

In what parts of the organization would it be beneficial to use resources? (Technology, processes, training or awareness efforts)

How should this be implemented in a small company?

Assignment given: 17. January 2007
Supervisor: Jan Arild Audestad, ITEM

Value of Investing in Information Security

A Metastudy Initiated by NORSIS, Gjøvik, Norway

Marie Kristin Johansen
<mariekj@stud.ntnu.no>

Teaching Supervisor:

Jan Arild Audestad
<jan-arild.audestad@telenor.com>

Advisors:

Tone Hoddø Bakås
<tone.bakas@norsis.no>

Tore Larsen Orderløkken
<tore.larsen@norsis.no>

May 31, 2007

Department of Telematics
Norwegian University of Science and Technology

Abstract

The ratio of companies and organizations in Norway with a number of employees between 5 and 9 and Internet access increased from 66% to 86% during a five year period from 2001 to 2006 [1]. This increased use of the Internet puts small companies (definition of small companies in section 3.1) in a vulnerable position considering information security. They are known to be remarkably less willing to pay for information security compared to companies with more employees and more revenue [2].

There is no such thing as two identical organizations. Every single one has it's own assets, weaknesses, employees and fundamental strategies. This makes each company's requirement for ICT-systems and information security identical as well. One solution might be good for one company but not for others. The differences in organizational structure and mentality is important variables in the process of building a good and secure infrastructure for the organizations.

The Australian Computer Crime Surveys [3, 4] presents four readiness to protect factors, they consist of: Technology, policies, training and standards. These factors are used as a template for this thesis. If companies focus on these four aspects of information security, and succeed in combining them in an optimal manner they are said to have security in depth. There is no use in investing great amounts of money on technology if these are not used in a justifiable manner. There might be several reasons for improper use of the technologies, among them; lack of knowledge, laziness and carelessness.

The companies continuous inability to calculate their own risks of adverse events and their total losses experienced due to computer crime makes it difficult to perform investment analysis on information security. Smaller companies do often have very limited amount of money to spend in general, and therefore also on information security. The investment analysis model chosen therefore take the maximum amount of spend able money into account. The accuracy of the model presented relies in the companies ability to present trustworthy data, and use both willingness to pay calculations and cost/benefit-investments analysis methods, resulting in a more thorough presentation of an ALE/ROI method used in a proof of concept using estimated data based on surveys, professionals experiences and prices used by a Norwegian ICT-operations company.

Preface

This report is the result of a master thesis written during the spring semester 2007 by one student at The Norwegian University of Science and Technology, Department of Telematics.

The objective of this thesis is to determine whether small organizations benefit from having good information security. The term good is relative and defined by me as the ability to provide security in depth. By performing quantitative analyzes on existing surveys, the main shortcomings in small organizations strategies towards information security will be mapped. An economical model for the investment analysis will be presented, with a following proof of concept using estimated data.

There are several contributors to this thesis. First of all I want to mention my teaching supervisor Jan Arild Audestad and advisors Tone HoddøBakås and Tore Larsen Orderløkken. They have provided useful input and constructive criticism to the thesis. Secondly, Kim Ellertsen for providing the complete data of the Norwegian Computer Crime Surveys (2003 and 2006). Lastly I want to thank Gaute Magnussen and Jan Ove Skogheim Olsen for useful discussions and providing help in correcting spelling and grammar errors.

Oslo, June 2007

Marie Kristin Johansen

Contents

List of Figures

Glossary

Authentication: A process used to verify the integrity of transmitted data, especially a message.

Ciphertext: The output of an encryption algorithm; the encrypted form of the message or data.

Cyber Terrorism: Terrorism that is directed at automated systems directly or that uses automated systems to disrupt other critical infrastructure systems that they support or control.

Cryptography: The branch of cryptology dealing with the design of algorithms for encryption, intended to ensure the security and/or autenticity of messages.

Digital Signature: An authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature guarantees the source and integrity of the message.

Directory Service: A directory service is a software application, or a set of applications, that stores and organizes information about a computer network's users and shares, and that allows network administrators to manage users' access to the shares.

DoS attack: Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

DSA: Short for digital signature algorithm. Algorithm used in digital signatures for autentication.

Firewall: A dedicatied computer that interfaces with computers outside a network, and has special security precautions built into it in order to protect sensitive files on computers within the network.

Hash Function: A funtion that maps a variable-length data block or message into a fixed-length value called hash code. The function is designed in such a way that, when protected, it provides an authenticator to the data or message.

Honeypot: A decoy system designed to lure a potential attacker away from critical systems, or to catch intruders by monitoring the honeypot.

Identity Theft: Identity theft occurs when somebody steals your name and other personal information for fraudulent purposes. Identity theft is a form of identity crime (where somebody uses a false identity to commit a crime).

Intruder: An individual that gains or tries to gain unauthorised access to a system or obtain unauthorised privileges on the system.

Intrution Detection System: A set of automated tools designed to detect unauthorized use of systems.

IPSec: Short for IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

Kerboros: An authentication service named after a three headed creature in greek mythology.

Malware: Malicious software.

Phishing: Type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, and other information.

Phishing filter: Phishing Filter offers dynamic new technology to help protect you from Web fraud and the risks of personal data theft.

Private key: One of two keys used in an asymmetric encryption system. For secure communication, the private key should only be known to the creator.

Public key: One of two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a private key.

Public-key Encryption: Asymetric Encryption.

RSA: A public-key encryption algorithm based on exponentation in modular arithmetic. It is the only algorithm generally accepted as practical and secure for public key encryption.

Smartphones: Mobile phones that permit users to install software applications from sources other than the cellular network operator.

Social engineering: In the realm of computers, the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information.

Spoofed Web Sites: Copycat Web Sites identical to the to the legitime sites, created for scam.

Spyware: Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.

TCP/IP: Short for Transmission Control Protocol/Internet Protocol, the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.

Trojan horse: A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

Virus: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

VPN: Short for virtual private network, a network that is constructed by using public wires to connect nodes.

CHAPTER 1
INTRODUCTION

The ratio of companies and organizations in Norway with a number of employees between 5 and 9 and Internet access increased from 66% to 86% during a five year period from 2001 to 2006 [1]. This increased use of the Internet puts small companies (definition of small companies in section 3.1) in a vulnerable position considering information security. They are known to be remarkably less willing to pay for information security compared to companies with more employees and more revenue [2]. The question is if this is a sign of lacking knowledge or a calculated risk these companies are willing to take.

1.1 RESEARCH GOALS

It is a lot of research on the field of information security today. This thesis is therefore concentrated around the smaller companies, and their fundamental needs in terms of ICT-security. This is a large group in the Norwegian population of companies, but is seemingly a bit forgotten in the ongoing research.

I have identified a set of questions to be answered in my project, these are:

- How are the smaller companies investing in information security today compared to the bigger corporations?
- What are the risks for smaller companies to experience adverse events and computer crime compared to the bigger businesses?
- Which threats to ICT-security are most common today, and which will be in the future?
- How much are small companies willing to pay for information security?
- How should small companies effectively secure their information with the money they are willing to spend?

The research goals for this thesis are the following:

- Give small business owners a manual and guidance in what factors they should take into considerations when attempting to secure their information.
- Provide a picture on the future of securing information, it is no use in believing that since you are secure today, you will also be tomorrow.
- Illustrate some issues that might not be considered as major threats, but might actually turn out to be some of the worst.
- Provide a simple but useful model on how to invest in information security.
- Give an example on how the model works in practice with estimated numbers.

1.2 Research Methods

I started my work by using the scientific method [21], observing the world using scenarios and proposing a model of theory of behavior. In the development of these approaches, the engineering method[21] was used, observing existing solutions, and purposing better ones. The approaches found where further applied to a concept case in accordance to empirical research methods[21].

The work can be divided in to four faces[22]:

- *The informational phase:* Gathering of information via reflection, literature survey, people/organizational survey or poll. I have mainly used other literature on the subject, and discussed the properties of the thesis with other persons, giving a clear picture of the issues at hand and background material on properties important for further development.
- *The propositional phase:* Propose and build a hypothesis, method or algorithm, model, theory or solution. I have proposed an approach to a modeling solution of the problem and how to perform the investing analysis.
- *The analytical phase:* Analyze and explore a proposal, leading to a demonstration and/or the formulation of a principal theory. In this phase I have used the approaches developed in the propositional phase in a example case with estimated numbers.
- *The evaluative phase:* Evaluate the proposal or analytical findings by means of experimentation or observations. The results developed from this phase are to be found in the discussion and conclusion part of the thesis.

1.3 Report Outline

The report consits of twelve chapters. These are:

- **Chapter 1 – Introduction**
  This first chapter discusses the project background, the motivation, research goals and the research methods used.
- **Chapter 2 – Scenario Planning**
  As a motivation for this thesis, a scenario describing possible outlook of the future concerning information security is used. The scenario are developed using qualified scenario modeling approaches appropriate for the different aspects of the future. The scenario developing models used are also briefly described.
- **Chapter 3 – Organizational Factors**
  The differences in companies in terms size, technical level of the employees, average age and other are important aspects to consider when looking at possibilities in security improvements in companies. In this chapter These factors are identified, and input are given on the characteristics of these companies in relation to information security.
- **Chapter 4 – Statistical Trends** This chapter presents results from a variety of different surveys on information security. These surveys are performed in different countries world wide and give a good description on how businesses handle information security and the development in recent years.

- **Chapter 5 – Information Security**
  There are a number of different technical threats and thereby also technical security measures companies might take to secure their information. This chapter presents some of the most usual information security technologies.

- **Chapter 6 – Mobile Threats**
  Some of the more unknown threats are found in the use of mobile devices. This chapter gives an introduction to the development in the threat levels for PDAs and smart phones.

- **Chapter 7 – Security Awareness**
  This chapter discuss the importance of the employee's ability to identify risks when using ICT-devices and applications, and how employers can prepare their workers in handling possible threats.

- **Chapter 8 – Security Management**
  It is important for the companies to have a clear picture of the value of their information. The managers are a big part of the effort of securing information, especially in smaller companies where there often are not dedicated ICT-personnel available. There are certain decisions and choices the managers might have to make. This chapter presents some of the issues a manager need to know about.

- **Chapter 9 – Cost and Value**
  Every benefit has it's price. The cost of introducing information security in different environments, and the beneficial outcome of the investments are presented in this chapter. A continuous example on how to use the presented method with estimated numbers will be given.

- **Chapter 10 – Discussion**
  This chapter discuss and summarize the results and information presented earlier in the thesis in relation to the research questions and goals of this project.

- **Chapter 11 – Conclusion**
  Concludes and presents results of my research.

- **Chapter 12 – Future Work**
  Suggestions on how this thesis can be taken further to improve the information security in smaller companies.

CHAPTER 2
SCENARIO PLANNING

This chapter will give an introduction to what kind of issues I will be dealing with throughout the entire thesis. To describe the issues I will utilize scenarios drawing on both science and the imagination to provide plausible accounts of alternative futures. They are credible stories about how the future might develop from the existing solutions, newly introduced factors and human decisions. In the stories it is possible to describe the future not only with words, but also numerical factors. The methods described later in this chapter give a wider picture, with more possibilities than mathematical modeling alone. Their simplicity also makes it understandable for a wider range of people. Scenarios bring possibilities to develop and illustrate the future pros and cons in a structured manner.

Scenarios are useful for my project because the information security problematic are evolving rapidly. There is an increased need for securing information. I will use scenarios to draw some outlines of how I see the future, and what challenges the future requirements of information security brings. I will use measured data from reliable statistical material in my work.

There are numerous approaches to scenario planning in use worldwide. I will first give a brief introduction to some of them, and then use these approaches to develop my own scenario of the future demand of information security.

2.1 THE BOGSAT METHOD

BOGSAT stands for Bunch of Guys/Gals Sitting Around A Table or Bunch Of Guys/-Gals Sitting Around Talking, which simply implies a meeting bringing nothing constructive to the table [1]. Scenarios are often developed in these settings. Subject matter specialists get together and discuss some topic, exchanges thoughts and work together developing scenarios. The BOGSAT method is often used as a starter for more structured approaches to scenario development.

The relaxed and nonformel atmosphere in this situation often works well as a brainstorming starter, to gather information from everybody around the table. The setting is not intimidating and the contributors might express ideas, which might not look important and relevant when first thought of , but with further discussion actually become key elements in the further development. The method is not recommended as the only part of a scenario planning process[5, 23]. Most of these processes will take form of a more structured model, in which I will describe some approaches to in the following sections.

[1] Acronym from http://acronyms.thefreedictionary.com/BOGSAT

2.2 SHELL SCENARIO PLANNING

Shell[2] have been working with scenarios for over 30 years and have developed their own map for successful use of scenarios. The scenario planning process is iterative process and intended to give strong implications to it's primary receivers. In scenario building their first step is to come up with focal questions, which define of the major challenges the primary recipients are most likely to face in the future. These questions should be asked in a way that allows exploration of critical uncertainties important to the recipients [24].

The next step in the scenario planning process is identifying branches. These are the different directions in which critical factors might play out. Each branch will provide an answer to the focal questions developed earlier in the process. The branches might also lead to new branches and develop into a tree structure.

The last is to develop the scenario outline, which actually is the story of the braches in the tree developed in the second step. You can develop scenario outlines from all the different paths in the tree or choose the most valuable or necessary ones. The story must be plausible, consistent and causal. The time span must not be long enough to let chaotic effects start to be significant. When you have developed a story, it is of great importance to be able to tell this story in a good manner. This can be by both oral or written presentation, but the important rhing is to keep the listener in mind when doing so.

2.3 COMPUTERIZED MORPHOLOGICAL ANALYSIS

Eriksson et.al. [5] describes Morphological analysis (MA) as a non-quantified modeling method for structuring and analyzing technical, organizational and social problem complexes. It is well suited for developing scenarios, and the method is described to be appropriate for complex cases where expertise from several areas is required. Read more about Morphological Analysis in [25, 26]. A morphological field is used to present the problem complex, its parameters and the conditions they can assume. A matrix is used to show alternative parameters, where a column represents each parameter, with conditions to the parameters in the rows below. The highlighted conditions are the relevant conditions for each parameter. In MA the configuration is denoted by X3-Y4-Z1. The parameters of each condition should be mutually exclusive. The findings of the configurations are often developed from many iterations, by assigning each of the conditions yes-maybe-no labels. When the configurations are determined, the scenario developing team should discuss alternative solutions and come up with a story concerning the configurations and its solutions.

2.4 THE PROJECT MOTIVATION USING SCENARIO PLANNING METHODS

In 1965, Gordon Moore observed that RAM memory size doubles approximately every 18 months. Computational power ($\sim$RAM memory times clock rate times hard disk size) doubles almost once a year. This is called Moore's law [27]. In later years Moore's law has not been an exact description of the computing power

[2] "Shell is a worldwide group of oil, gas and petrochemical companies with interests in biofuels, wind and solar power and hydrogen." www.shell.com

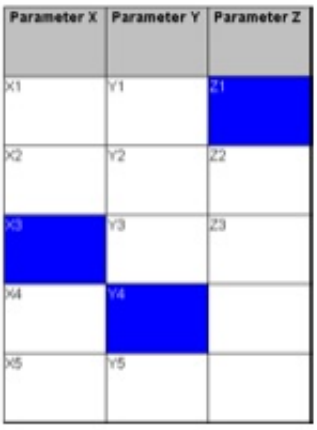

Figure 2.1: Description of a MA matrix for presenting the different parameters and their conditions[5].

development, but is still assumed to be quite accurate. This means that the price to maintain, process, and communicate information is nearly cut in half every two years.

The empirical truth of Moore's Law the past four decades has forced firms and organizations in all industries to maintain, communicate and process increasingly more information. They have been forced to invest increasing amounts of money developing information systems, to be stay competitive with their rivals in the market.

The increased information flow includes information valuable to the companies. Information that should not be in wrong hands. The information therefore needs to be secured and managed with great care. There are differences in information value. Not only in different industries, different companies and organizations, but also within the same computer and information infrastructure.

2.4.1 The BOGSAT Approach

In 2.1 I have explained the simplest scenario planning method there is. I've started out with this method, explaining and discussing my thesis with a number of different people, mostly in some sense experts or qualified expertise in computer technology and communications technology. I simply asked questions on how they saw the future, and what problems they thought where important to take notice of. Most of them had strong opinions on the matter. The persons where not asked to be quoted on their statements, so they will remain anonymous. Some of the statements where:

> "I believe the most concerning issue is the increase in mobile use beyond conversations. Take for instance Bluetooth, there are a lot of people carrying vulnerable information on their cell phones and PDAs not knowing Bluetooth is on, creating an open gate to information. Bluetooth on cells might be the next step in distributing viruses"

> "There are so many different needs for information security, probably one for every company there is"

”There are no such thing as being secure from intruders or other unexpected and unwanted incidents. The only thing one can be is ”secure enough”, to a certain extent.”

”The key to security is security in depth. There is no use in applying security measures in some stages of a process if other stages are unprotected. You are only as strong as your weakest link”

All of these conversation gave great input to further scenario planning, helping to find good focal questions and pinpointing the biggest concerns among professionals in the information industry.

2.4.2 The User Scenario

The results of surveys, mapping the incidents in information security breaches during the last year, helped me find useful information about the users mindset. The first four columns in the Morphological Analysis matrix represent the four readiness-to-protect factors; Technology, policy, standard and training introduced by the Australian Computer Crime Surveys [3, 4]. These data are inspired by the survey results [6, 4, 9, 28, 3, 7], described in chapter 4. For this scenario I have chosen to use MA-methods, see 2.3 for this scenario description because this method often has been proven to work well for social dependent scenarios [5].

I first made a Morphological Analysis matrix that gives seven parameters, and

Information security budgeting	Training of employees	Use of standards	Use of policies and practices	Users knowledge	Users awareness	Information security management
None	No IT training	No use of standards	No use of policies	More knowledge in general staff than today	More aware than today	No experts in companies
Up to 5% of IT budget	<20% have proper staff training every two years	<20% use standards	<20% have policies	More knowledge in management than today	Less aware than today	Own employees with expertise
5-15% of IT budget	20-50% have proper staff training every two	20-50% use standards	20-50% use policies	Less knowledge in general staff than today	Do not care about security	Outsourced IT
>15% of IT budget	>50% have proper staff training every two years	>50% use standards	>50% use policies	Less knowledge in management than today	Thinks information security are annoying	Managed Security Services

Figure 2.2: Morphological scenario planning with user perspective

different outcomes or conditions of these parameters. The most likely outcome, as I see it, is highlighted with a blue background color in Figure 2.2. As you can see I predict no large improvement in the attitudes towards information security for smaller companies. Business will not start spending more money on security measures, few companies training their staff, between 20% and 50% use of standards,

which is an increase from today, and I also believe we will see an increase in the use of policies and best practices.

I believe the managers in smaller companies will know less about information security than they in general do today. At the same time I think the over all work staff will become more educated in this area. The reason for this is the fact that managers have a lot to do, and the amount of tasks they have increase. Managers are often well educated people that probably did well in most departments prior to their advance, including information security. However, the rapid change in the attackers strategy and technology makes me believe that management in businesses do not have time to catch up. Due to the new digital generation where youngsters practically grow up with their computers as their best friends, the average Joe will know more about technology than the workforce do today.

The ongoing trends in security awareness will just keep on. Unless, off course, we experience some serious losses due to ignorant behavior. The general workforce continue to see information security measures as annoying, despite their increased knowledge of the computer industry and technological finesses. As I see it, managers that can not keep up need to delegate work surrounding information security. Even though this scenario planning method suggest you choose one or two of the outcomes, I felt this was not possible for the parameter. There will probably be as many ways to organize information security management as there are businesses. However, to get the whole picture it is important to consider how the attackers will behave in the future.

2.4.3 The Attacker Scenario

The scenario planning used by Shell, see section 2.2, is often used to create scenarios for situations where the future choice of technologies is not obvious. I have therefore chosen to use this this approach. I started the scenario building by finding a focal question:

- Why and how will attackers intrude and abuse systems or equipment in the future?

The next step is to make branches from the question, suggesting answers to them. This is done in Figure 2.3. By choosing some of these branches I am able to form a scenario, describing my view of the future.

Looking at the development the last years might bring some clue to how the development will be the next years. The surveys studied later in this thesis give a good picture of the reality of this question today and how it has developed the resent years. My thoughts are therefore closely connected to these results. There are mainly three reasons why someone would like to commit computer crimes. There are hackers doing this for prestige and for the laugh of it, there are people trying to scam people for money, and lastly there are people who is after information. These three groups of criminals used to be of the same threat level. This is no longer the case. We see more and more professional people, also inside the companies performing organized computer crimes to gain valuable information. This information gained is used for all it is worth, and the outcome can be enormous. I also believe there will be an increase in theft of equipment, and scams online to steal money. The traditional hackers however, I believe will fade out in the company of organized fellow criminals.

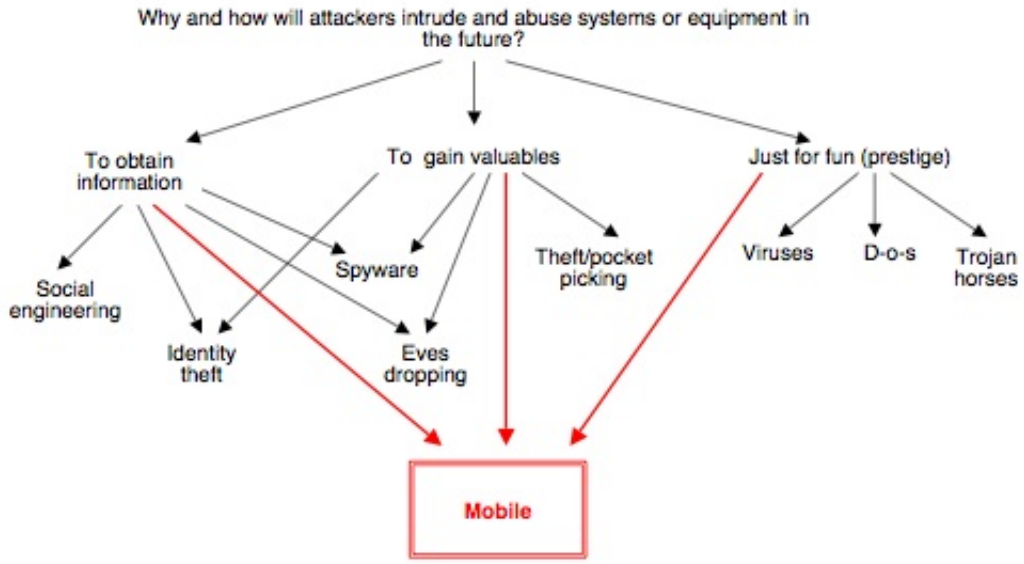

Figure 2.3: Focal question for the attacker scenario

There is one key point highlighted, see figure 2.3 when it comes to the matter of how these crimes are performed. This is mobile threats. We have yet to experience huge attacks via portable equipment, such as mobile phones. More and more of our valuable information is accessible also from these devices. However, other types of attacks I believe we will se more of in the future are:

- Theft of money (often very small amounts from several accounts)
- Theft of information
- Warfare
- Terrorism
- Identity theft
- Social engineering
- Spyware
- Evesdropping

I am not sure if the amount of Virus/worms attacks will decrease but I do not think this will be among the biggest challenges in the years to come.

2.4.4 The Project Motivation

There are obviously an enormous lack of respect for information and it's value. Not only do companies spend little money protecting their information, the average Joe is also lazy. We do not want to spend an extra second, even though this actually might save the company or ourselves a lot of money. An extra policy is not welcome

at all. This combied with the lack of knowledge about technology, the risks encountered and the value of information presents a risk in today's reality of possible threats.

Can these problems be solved by throwing money at them? Is it possible to pay to change your employees attitude towards security? Smaller companies might not benefit from spending enormous amount of money on super fancy technology. It is necessary to do risk evaluation and map the possible losses due to adverse events to determine the benefit of the investment. Would anyone care to spend time and money to break into our systems? Is the valuable information available other places? In some respects the attackers have the same attitude as the businesses. They brake to profit, and if it costs more than it tastes, they simply will not do it.

Spending money on technology is a total waste if the users do not know how to use it or they just do not bother to. There are also a lot of cases where the attacker actually is a trusted employee. If a user has access to the information, the individual can choose to take advantage of this despite technology. It all comes down to attitude, you need security in depth to be able to shake of intruders.

CHAPTER 3
ORGANIZATIONAL FACTORS

To understand and analyze the need of information security it is important to take organizational properties into account. Different types of organizations need different security functionality based on the level of information value located in the organizations networks. In this section I will try to differentiate organizations into categories important for further evaluation of investments in information security.

3.1 SIZE OF ORGANIZATION

The thesis will mainly be looking at small businesses and organizations. This term is a matter of individual consideration and varies greatly in different countries and regions. First there will be given an overview of different definitions, and then present the one I want to use throughout this thesis.

3.1.1 Definitions

In the U.S the SBREFA[1] references the definition of "small business" found in the Small Business Act. The Small Business Act further authorizes the Small Business Administration (SBA)[2] to define "small business" by regulation. The SBA's small business definitions are codified at 13 CFR 121.201. The SBA defines small business by category of business using North American Industrial Classification System (NAICS)[3]. For example, in the case of manufacturing, generally defines small business as a business having 500 employees or fewer. For many types of manufacturing, however, the SBA's size standards define small business as a business having up to 750, 1000 or 1500 employees, depending on the particular type of business.

In Europe the European Commission has one definition of very-small (micro) enterprises and one of small ones. The definitions can be found in table 3.1.

Statistics Norway [4] also provides a definition commonly used in Norway. This definition uses considerably less employees than the other ones I have presented. A company is considered to be small only if there are less than 20 employees. Companies with more than 100 employees are considered large. Norwegian Laws provided by the Norwegian Ministries [5] are however in most cases obligated to use the EU

[1] Small Business Regulatory Enforcement Fairness Act of 1996

[2] The U.S. Small Business Administration (SBA) was created in 1953 as an independent agency of the federal government to aid, counsel, assist and protect the interests of small business concerns. Read more at: http://www.sba.gov/index.html

[3] NAICS is a unique, all-new system for classifying business establishments, used by the statistical agencies of the United States. Read more at: http://www.census.gov/epcd/www/naics.html

[4] Reed more at: http://www.ssb.no/english

[5] http://www.regjeringen.no/en

Criteria	*Micro*	*Small*
Number of employees	Less than 10	Less than 50
Annual turnover or global balance	Less than 2 million euros	Less than 10 million euros
Independence	In principle	Not exceeding 25% of the capital or voting rights withheld by one or more companies (or public bodies) which are not them selves SMEs

Table 3.1: The European Commissions definition of small companies []

definition. This is due to the Norwegian membership in EFTA [6].

3.1.2 My Definition

The differences experienced in these definitions are not surprising, due to the huge difference in number of citizens in the different regions. Taking the three definitions into considerations I have decided to use a definition where companies with less than 50 employees are considered small. I will also divide this into three smaller categories shown in table 3.2. The reasoning for this categorization is to both be to

Criteria	*Micro*	*Mini*	*Small*
Number of employees	Less than 5	Less than 20	Less than 50

Table 3.2: My definition of small companies used in the thesis

use the European standard and at the same time take Norwegian proportions into account. The quote *"One of three Norwegian companies are small companies with the owner as the only employee."* [29] indicates that the Norwegian organizational structure probably is quite unique when it comes to size. These companies are probably some of the most vulnerable companies when it comes to information security because of ignorant behavior. Small companies do often not expect malicious intruders to show interest in their network or information, which is one of the most common and dangerous mistakes one can make. Johnson et.al. [8] illustrates the concurrent lack of knowledge among small home-based companies when it comes to securing their information. These mini-companies are therefore of particular interest throughout the thesis.

It is also important to divide the number of employees into intervals that can be easily associated with different ratings of the other organizational factors described later in this chapter.

3.2 TECHNICAL SKILLS

There will of course be differences in the level of technical skills in companies. This might be related to the actual size of the company, but not always. It would be

[6] European Free Trade Association, http://www.efta.int

interesting to see if the internal ICT-competence in companies is decisive for the information security levels and if this infulence the choices of security measures. This section define companies with different internal technical knowledge.

3.2.1 ICT Companies

This category contains the companies working in the following business areas:

- Electronic education
- E-commerce
- Remte sencing and control
- Software development
- Teleoperators (powning infrastructure, virtual operators, resellers)
- ICT consultant services
- Network providers
- Network/software maintenance
- Tele and Computer stores
- ICT security
- Computer production

There is no requirement for people working in the companies to have any kind of education within ICT. The only common property of these companies are that they in some way provide ICT services to customers, either other companies or private households. In some way they should therefore be aware of the threats connected to ICT. One might think that companies that daily produces ICT systems or build network for customers are more aware of security breaches experienced in ICT systems and networks and therefore protect their own information better.

3.2.2 Companies Not Delivering ICT Services

This category represents all companies not delivering ICT services and is therefore huge. It might have been beneficial to place other technical companies in a separate category because one might expect such companies to have slightly more insight in ICT difficulties than others. I have however chosen not to, because I believe the differences would have been microscopic. There would also probably have been extreme differences depending on their technical area.

3.2.3 Companies With ICT Department

The slightly larger companies will in some cases have dedicated ICT departments taking care of the internal ICT systems. The companies I will be looking at will in most cases not have this kind of competency. Some of the companies in the small company category described in 3.1.2 might however have their own ICT-department. The smaller companies might also have one of their employees assigned to take care of the internal ICT systems. I will categorize these as companies with their own ICT department.

3.2.4 Companies Outsourcing The Responsibility Of ICT Maintenance

Some smaller companies find it beneficial to hire external resources for ICT maintenance. Such external resources are often companies categorized in the first category described in 3.2.1. This is getting more common also for larger companies, but are first and foremost useful for vulnerable small companies that can not afford hiring their own dedicated ICT personnel.

3.3 Information Value

There are different level of confidentiality, accessability and integrity necessary for different companies and business areas. There might also be different needs within a single company. I will in this section try do differentiate companies on a classification of high, medium and low level information vulnerability. This differentiation is mainly based on the probability of economical loss since the thesis' focus is on the economical aspects of information security.

3.3.1 High-level Companies

In this category one typically finds companies that are dealing with patient or client confidentiality required by law. These companies need to have a minimum level of security when storing classified information digitally. By neglecting to do this they might loose their to do business. Business areas obligated to keep information classified by Norwegian laws are:

- Health (Doctors, nurses, psychological personnel etc.) [30, 31]
- Financial institutions [31]
- Police [32, 33, 31]
- Lawyers [34, 33, 31]
- Government, when information is personal, involves other peoples business secrets, endangers the nations safety or the information is obtained in the line of duty. [35, 36, 31]

3.3.2 Medium-level Companies

Companies that might suffer severe economical losses if their information get in to other people hands are placed in this group of information vulnerability level. This is for instance information on possible patents or information that harm the companys reputation. This includes business areas such as:

- Research
- Petroleum
- Restaurant
- Pharmaceutical companies
- Textile

3.3.3 Low-level Companies

All companies experience some risk of loosing information to malicious intruders. In this group however, the information will not lead to losses that jeopardizes further activity in the company. There is no high-risk information that might lead to severe losses in company value. These companies might be the same as mentioned in subsection 3.3.2; specially if they do not have any production secrets harmful to their reputation.

CHAPTER 4
STATISTICAL TRENDS

I have used statistical material, gathered by several different agencies. For Norway I have used surveys from statistisk sentralbyrå(SSB) and næringslivets sikkerhetsråd (NSR). These numbers give answers and indicate the main trends concerning information security in Norway.

I have also studied the Australian Computer Crime and Security Survey for 2004 and 2006. This survey is administrated by the Australian Computer Emergency Response Team (AusCERT). Lastly I have also considered the Computer Crime and Security Survey from the United States, published by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) in 2005 and 2006. None of the above mentioned surveys cover all of the interesting aspect for this theses. I will therefore use them to complement and verify each other.

In this chapter I will describe the statistical findings in terms of how companies ICT-systems are attacked, which measures the different companies take in terms of both technical and organizational assurance and how the companies handle the attacks when experienced. I will also look at the amount of money organization spend on information security.

4.1 ATTACKS

In this section I will take a look at the statistical trends in terms of successful and attempted attacks. I will first look at the results of the earlier surveys [6, 4, 9] and then the most recent ones [28, 3, 7]. In 4.1.3 I will look at the development in attacks on ICT-systems the last few years.

4.1.1 The 2003-2005 Surveys

The survey [6] do not only cover data crime but all unwanted and unexpected ICT-situations. 60% of Norwegian companies experienced such situations in 2003. This includes:

- 5200 data break-ins
- 2,7 mill. attempts of data break-ins
- 150 000 virus attacks
- 50 mill. attempts of virus attacks

Only 50 of the data break-ins were reported to the police or other federal agencies.

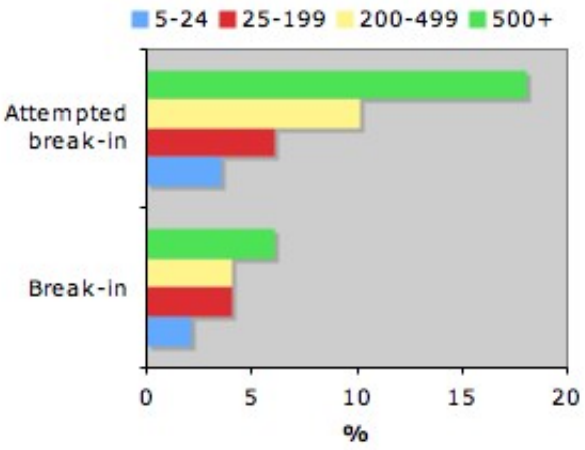

Figure 4.1: Differences in attempted and successful data brake-ins for companies of different sizes [6].

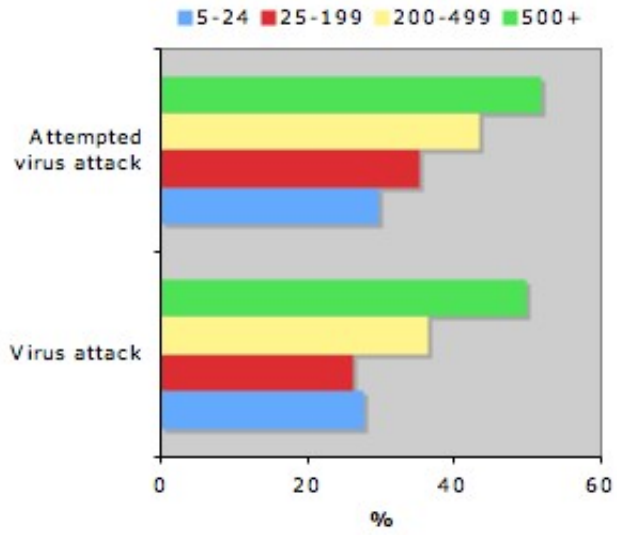

Figure 4.2: Differences in attempted and successful virus attacks for companies of different sizes [6].

The results in [6] show that larger companies are less likely to experience theft of ICT-equipment and abuse of ICT-resources. About 2% of all companies have had information stolen from their systems in 2003. Attacks on smaller companies computer systems do however seam to be more successful than attacks on bigger ones. This is not surprising since smaller companies seam to spend less effort and money on protecting their computers, networks and information. See figures 4.1 and 4.2. There are systems for detecting break-ins. 20% of the big companies do have this functionality, while only 6% of the small ones do.

Both thhe Australian and US survey back up these results.

4.1.2 The 2006 Surveys

[28] indicates that 40% of Norwegian companies have had incidents where they where victims of ICT-crime in 2006. This number does not involve attempted attacks that are unsuccessful. About one third of the companies do not know if they have had break-ins the last year. The most frequently reported incidents in [28] are:

- virus attacks
- theft of ICT-equipment
- misuse of ICT-resources

Almost all the asked companies use authentication and anti-virus solutions.

In 2006 the Australian survey [3] showed a great decrease in incidents (now only 22%). This is much lower than both Norwegian results and the results from the US computer crime survey (53%), see table 4.1. The possible reasons for this is interesting to look further into. This might be because of some findings in section 4.3 where the trends in Australia seamsto be increased used of standards, policies and procedures.

4.1.3 What has Happened? 2003 - 2006

In [3] there are reported that 1 out of 5 companies experienced electronic attacks that harmed the confidentiality, integrity or availability of network data or systems during the last 12 months. This is substantially fewer than in the last three years. The Norwegian numbers are also decreasing, but this might be due to the fact that in 2006 these numbers only represented the successful attacks, not all of the attempts. There is also a slight decrease in the USA, where there is less total economical loss than the year before[7].

	$Norway$	$Australia$	USA
2006	40%	22%	52%
2005	-	35%	56%
2004	-	49%	53%
2003	60%	42%	-

Table 4.1: The percentage of companies that have experienced unauthorized use of ICT-systems the last year.

4.2 TECHNICAL SECURITY MEASURES

Similar to the previous section, I will take a look at the statistical trends in terms of the technical security measures taken by the organizations. I will first look at the results of the earlier surveys [6, 4, 9] and then the most resent ones [28, 3, 7]. In 4.2.3 I will take a look at the development in the use of technology to prevent attacks on ICT-systems the last few years.

4.2.1 The 2003-2005 Surveys

Wireless networks are used at an increasing rate, but more than 30% do not use encryption for securing the transferred data. Every third company admit to being slow in applying security patches for their applications e.g. their anti-virus programs[6].

Great amounts of private information about patients are stored in the health- and social- organizations data systems. It is therefore quite alerting that half of the businesses in this sector do not know whether they have had any information stolen or if their systems have been broken in to. These businesses also uses encryption to a smaller extent than the average business do (only 13%). In bank and finance almost 40% use encryption [6].

In 4.3 one can see that passwords, anti-virus programs and firewalls are used by almost all of the Norwegian companies. The numbers are however substancialy lower for the smallest companies.

The results from the Norwegian survey are backed up by the Australian and US when it comes to technical assurance. The same mechanisms are used by approximately the same amount of companies.

4.2.2 The 2006 Surveys

One of the most alerting findings in [28] is the fact that only 11% of the companies are encrypting the discs on portable equipment. Considering that theft of these units is one of the highest rated on the attack statistics this result might seem a bit surprising.

Smaller companies are also reported to be slow in taking spam-filters in use. Companies with less than 25 employees have this technology in 62% of the cases. This despite the great value of these filters in terms of effective use of e-mail and limiting the spreading of malicious code [28]. The use of UPS and backup power is common in larger companies. Unfortunately, also in this case the smaller companies fall behind.

4.2.3 What has happened? 2003 - 2006

In [6] only 62% of the smaller companies used firewalls. In three years this number has increased to 83%. Despite the firewalls need for frequent updates, only 15% of the companies report that they have routines for this [28]. There has also been an increase in use of backup in small Norwegian companies. 83% are now using back-up, compared to 73% in 2003 [28].

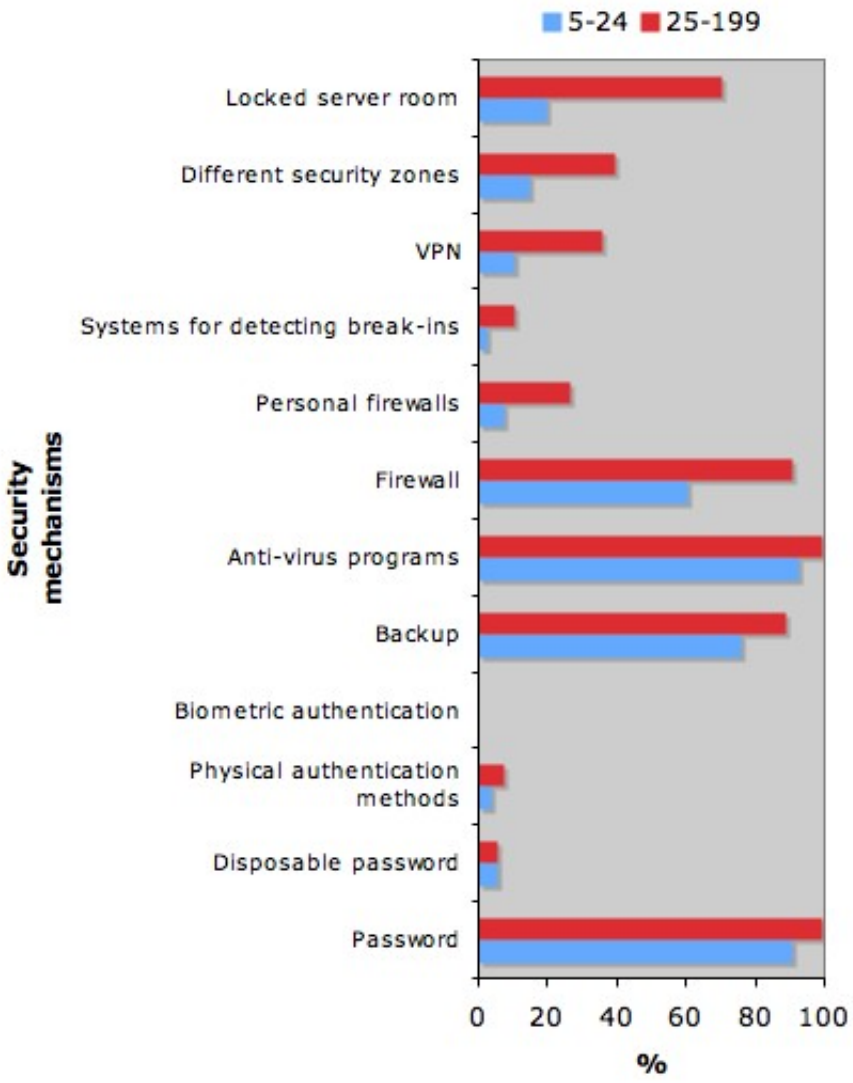

Figure 4.3: Overview over in what extent security mechanisms are used in small and medium sized companies [6].

There is an increase in the use of disposable passwords. This is especially a trend for the smallest companies (1-5 employees) where now 16% use this technology. There is also increased use of Personal firewalls which should be seen in context of the Microsoft Windows XP Service Pack 2 release where this is an integrated feature.

4.3 Organizational Security Measures

It is worth noticing that the Norwegian 2006 Computer Crime Survey, [28] reports that of the companies who have experienced attacks the last year, 97% had anti-virus programs, 86% had spam-filters and 94% had firewalls for their network. This indicates that technical measures alone are not enough to avoid unpleasant incidents. Similar to the previous two sections, I will look at the statistical trends in terms of the organizational security measures taken by the organization. I will first look at the results of the earlier surveys [6, 4, 9] and then the most recent ones [28, 3, 7]. In 4.3.3 I will look at the development in investments in organizational efforts to prevent attacks on ICT-systems the later years.

4.3.1 The 2003-2005 Surveys

The Norwegian survey [6] does not contain any data on this matter. The Australian computer crime survey [4] does however give indication on increased use of Computer security policies and procedures. Since 2003, there has been a small but consistent increase in the use of these measures in most categories. This is positive indication that there is greater recognition of the importance of having appropriate information security policies and procedures in place to more effectively manage network security. The biggest increases were in the use of incident management procedures (from 51% in 2003 to 64% in 2004); and procedures for defence against malicious software (from 62% to 72%).

[4] also reports a positive development in the use of ICT security related standards from 37% in 2003 to 58% in 2004. Information security standards provide a framework from which to develop information security policies, practices and procedures tailored to an organizations risk requirements.
A sizable majority of the respondents organizations (69%) report that their ICT security staff did not have sufficient experience and skill to meet their organizational needs. This despite the fact that trained and certified staff has increased. This is probably a direct effect of the increased used of standards, policies and procedures which brings awarenss to businesses. Respondents also expressed significant concern about the adequacy of awareness training for general staff and management; 85% and 80% respectively as seen in figure 4.4.

4.3.2 The 2006 Surveys

In the incidences where the perpetrator is identified, almost half are employees or hired help at the affected company. This shows that focus on attitude towards information security might be worth spending money on. None the less, just 40% of the companies with under 200 employees have specified agreements on information security when outsourcing the ICT-operation [28]. This is not however backed up by the Australian surveys, which reports that approximately 36% of the attacks are

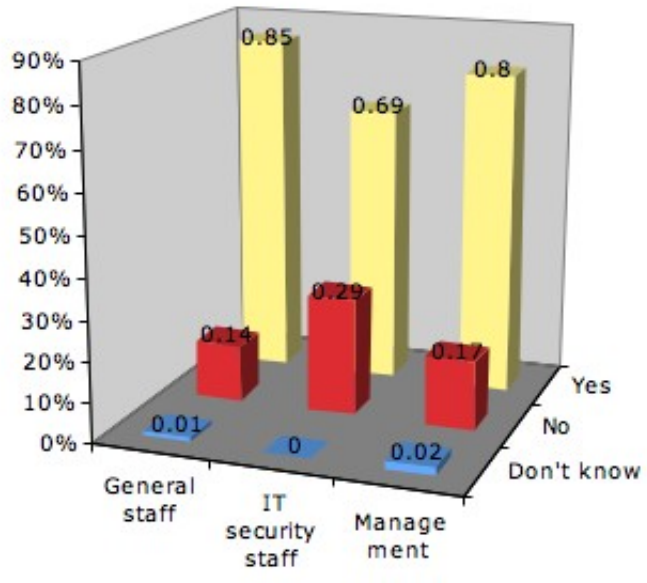

Figure 4.4: Results from the question: Do you think you organization needs to do more to ensure an appropriate level of ICT security qualification, training, experience or awareness for general staff, ICT security staff and management? [4].

performed by company insiders. In the US survey however, 39% of the companies have estimated their loss due to illegal operations by an inside person to be over 20% of the total loss 4.5. The Norwegian results might be slanted by very few reported incidents, and even less cases where the perpetrator actually was identified. It might be easier to find a local source of crime than an external one.

Among smaller companies only one of four have policies for the employees use of ICT. This is a lot less than the bigger ones, where almost all of them state that they do have these kinds of policies. In [28] 83% of the answers state that they frequently or sometimes evaluate the risk and need for security measures. 17% say that they never or seldom do this.

In [28] only 40% of the companies have had some kind of training of their employees in secure use of ICT.

4.3.3 What Has Happened? 2003 - 2006

There are four so-called readiness to protect factors:

- technologies
- policies
- standards
- training

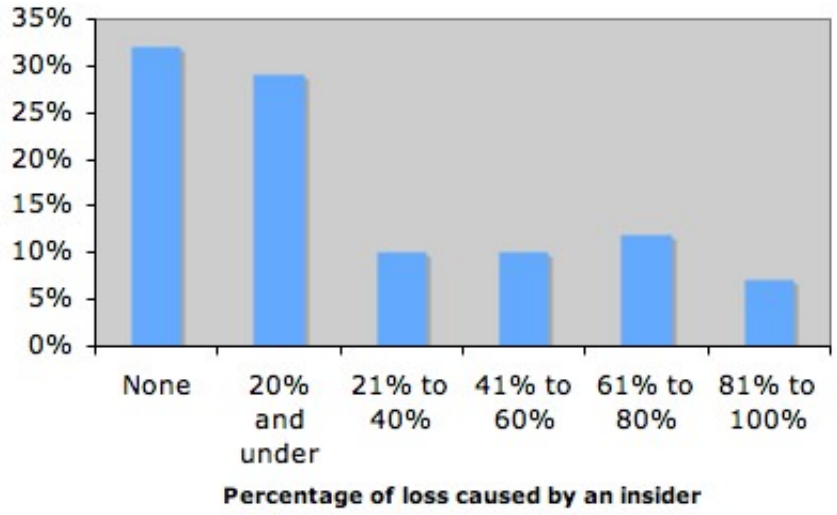

Figure 4.5: From this chart you can see that employees are estimated to cause employers great expenses due to computer crime [7]

Among the four readiness-to-protect factors perhaps the most significant downward trend in [3] is the proportion of organization that use or follow various ICT security related standards. There was more focus on this measure in earlier years in Australia and this might be the reason why they have the most optimistic statistics when it comes to incidents of ICT crime. In 2006 the share of companies that use policies was down to 47% compared to 65% as an all time high the previous year.

There has been a downward trend in the percentage of the respondents that have ICT or ICT security qualifications or training across various categories. At the same time, less respondents report that their staff members need to undergo more training to ensure that their level of competency is good enough, figure 4.6. This number is however not much lower than the year before (68% and 65%).

4.4 Cost Of Attacks And Investments In Information Security

In this section I will take a look at the statistical trends in terms of the organizations efforts to estimate and calculate the loss when attacks occur. I will also look at the development in organizational ability to measure actual loss when an attack on ICT-systems occur.

4.4.1 The 2003-2005 Surveys

The 2003 Norwegian survey show that it is very hard to estimate the total loss resulting from computer crime and other unwanted events. Only 25% of the businesses in the study were able to estimate the direct loss due to such events. Even less (only 6%) managed to estimate the indirect losses. Of the companies that where able to calculate the amount of loss, the average loss where approximately NOK200.000 in direct costs and NOK400.000 in indirect costs. Only 12% of the

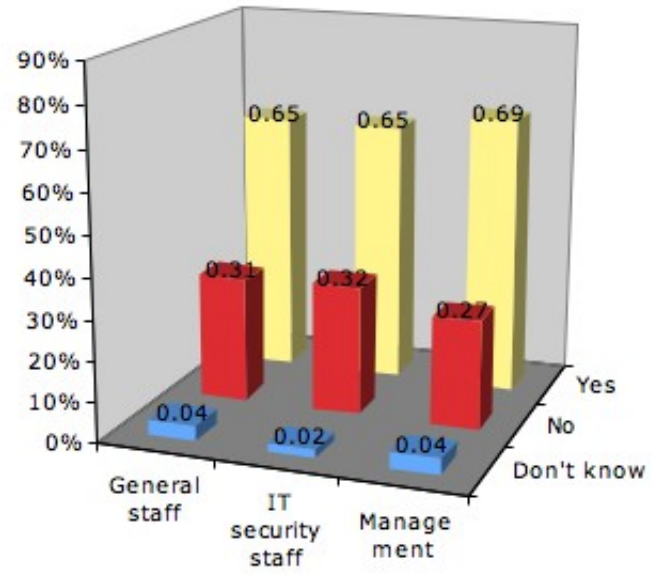

Figure 4.6: Results from the question: Do you think your organization needs to do more to ensure an appropriate level of ICT security qualification, training, experience or awareness for general staff, ICT security staff and management? [3]

respondents have routines for estimating their losses. This indicates that the costs of security breaches are not yet in focus. See more about the development of these losses for American companies in section 4.4.3

Out of all the companies that have had unwanted experiences in 2003, 70% reported that they had encountered extra work due to the event. Nearly 40% reported that they had their security up for evaluation after the incident. Nearly 5% meant the incidents led to loss of business and 2% was scared that their credibility was compromised due to the event, see table 4.2.

One question introduced a year ago was aimed at determining the typical size of

Result	2001	2003
Extra work	65%	69%
Evaluation of security	31%	38%
Loss of business	2%	5%
Compromized credibility	3%	2%
None of the abow	9%	5%
Other	-	2%
Don't know	-	1%

Table 4.2: Outcome of unwanted information security incidents.

an organization's information security budget relative to the organization's overall ICT budget. 48 percent of respondents indicated that their organization allocated between 1 percent and 5 percent of the total ICT budget to security. Only 11 per-

cent of respondents indicated that security received less than 1 percent of the ICT budget, 27 percent of respondents indicated that security received more that 5 percent of the budget, while 15 percent of the respondents indicated that the portion was unknown to them. A comparison with the 2004 results shows that there is essentially no change in the percentage of the ICT budget allocated to security [9].

4.4.2 The 2006 Surveys

Companies are getting more and more dependant on ICT. Almost all companies use e-mail. Four out of five have got their own web site and pay their bills electronically. Bigger companies seems to be faster in taking new technology in use than smaller companies. This is reflected by the fact that bigger companies often are the first to experience new attacks, and are generally more vulnerable to adverse events.

In [6] two of three companies report that they will encounter substantial problems if the most important ICT-systems are down for more than one day. Eight out of ten companies have stored essential information electronically and nine out of ten will encounter great problems if their information is not trustworthy or incorrect. It is therefore surprising that only one in four companies where able to estimate how great their losses were. Only 12% had routines to measure their losses when attacked. The reported losses will be discussed in greater detail in section 4.4.3

Looking at some exact numbers from the American and Australian surveys, one find that only about half of the companies spend more than five percent of their ICT budget on information security. The businesses with the lowest organization revenue, are the ones spending the most on information security per employee. This might be because of higher fixed costs, but it also seems they spend more on awareness training ass well. These cost are mostly based on training fees, which are variable costs based on the number of participants.

Johnson and Koch provided an interesting proceeding on the 39th Hawaii Interna-

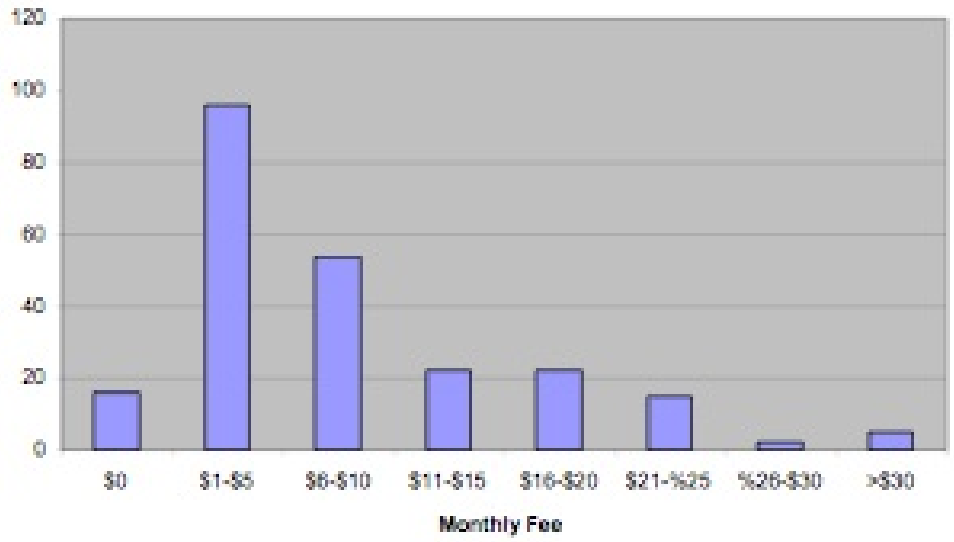

Figure 4.7: Results from the question: How much would you be willing to pay for a service protecting you from all information security threats on the internet? [8]

tional Conference on System Sciences 2006 [8] taking on the lack of information security knowledge at home-based small business owners. As part of the survey, respondents were given the description of a comprehensive security service that protected them from all the Internet-based threats discussed earlier in the survey, such as Virus attacks, spyware, trojan horses, spam and pop-ups. When asked to rate their interest in such a service, respondents averaged 5.93 on a 7-point interest scale. 47% were Extremely Interested (7) and 87 percent expressed a High interest (5, 6, or 7). When asked if they would subscribe to such a service, the results were as follows:

- 22% of the respondents indicated that they "Definitely would subscribe"
- 43% indicated that they "Probably would subscribe"
- 31% indicated that they "May or may not subscribe"

Figure 4.7 shows what the respondents felt such a comprehensive security service would be worth as a monthly fee. If one uses the midpoint of the ranges to calculate an average monthly cost that respondents were willing to pay for an ideal protection service the result is a mere $8.55.

4.4.3 What has happened? 2003 - 2006

According to [7] respondents' estimates of the losses caused by various types of computer security incidents dropped significantly from 2005 to 2006. This is in fact the fourth consecutive year that these loss estimates have dropped. Indeed, while this year's decline is significant, it is the smallest percentage drop of the four years. Total losses for 2006 were $52,494,290 for the 313 respondents that were willing and able to estimate losses, down from the $130,104,542 losses for the 639 respondents that were willing and able to estimate losses in 2005. Much of the decrease in total losses is easily explained by the fact that the number of respondents willing or able to report their losses this year was less than half of the previous year. This might indicate that use of procedures to calculate losses have decreased. Nevertheless, there appears to have been a real decline, as the average loss per respondent decreased nearly 18 percent from $203,606 to $167,713. These numbers are a bit larger than the numbers for the Norwegian companies described in 4.4.1, but the indications are the same .

As you can se in figure 4.8 there is an increase in people spending less than 2% of the ICT budget, but at the same time also an increase in those spending more than 5%. This is an obvious trend of a greater gap between the companies willingness to pay for information security. The leaders are most likely to be involved in the budgeting process and the gaps might indicate a gap in the leaders knowledge about these issues. Another thing this might indicate is the fact that the organizations most likely to be hit by unwanted incidents, increase their economical effort to avoid it.

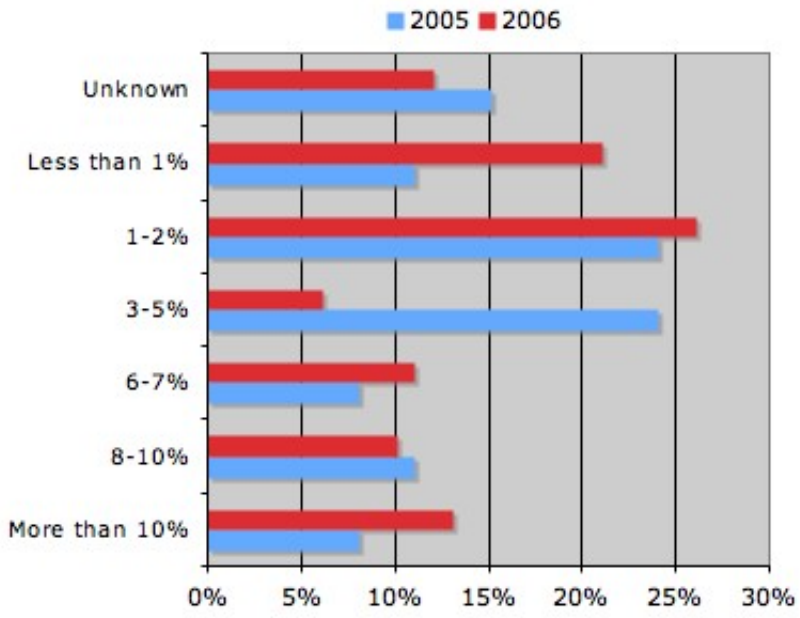

Figure 4.8: Results from the question: In the past 12 months, what proportion of your ICT budget was spent on ICT security? [7, 9]

CHAPTER 5
TECHNICAL APPROACHES

Arora. et.al. [37] compares the situation regarding information security to the state of medical practice in the 19th century. Medical practitioners had a poor understanding of the prevalence, likely outcomes of illness causes, and the safety and effectiveness of treatments. The human body was to complex to understand (to some extent still are today), and the population feared treatments, and thought of it as ineffective. Today the medical business is clearly different. The medical advertisements are regulated, and it is necessary by law to inform about side effects, effectiveness and other properties of the medicine. If these properties where not stated, the people would probably take it all. It will be exiting to observe if the information security business will follow some of the same trends.

Table 5.1 present the use of information security efforts percent og Norwegian companies with more than 10 employees in the years 2003 – 2006. It is reason to believe that statistics only for companies with less than 10 employees would be even more concerning, unfortunately this is not available. The reason for this is that smaller companies seems to have very small if at all existing budget for information security. In this chapter I will concentrate on the technological aspects of information

Security effort	2003	2004	2005	2006
Digital signature	10	6	7	9
Other methods for identification	13	10	13	11
Encryption of information	8	7	11	10
Physical delimitation of critical ICT equipment	31	36	49	50
Emergency power system	38	36	46	45
Back-up outside the system environment	63	61	68	71
Server with secure communication (SSL, HTTPS etc.)	26	33	51	57
Firewall	54	66	80	86
Virus control and security programs	81	85	88	90
Running subscription of security services (anti-virus etc.)	57	68	82	78
Continuous education in ICT-security of employees	14	13	23	34
ICT-safety policies accepted by the company leaders	-	23	46	45
Announced one responsible employee for the ICT-security	-	28	39	39
Emergency plan updated in the last two years	-	14	27	27
Updated ICT-safety guidance for all users in the last two years	-	12	25	23
Filtering incoming e-mail (anti-spam filter)	-	44	70	77
Updated any safety efforts within the last three months	70	81	82	86

Table 5.1: The information security efforts used in companies in percent in the years 2003 - 2006. [38]

security, while chapter 7 will consider the “softer” efforts.

5.1 FIREWALL AND VIRUS CONTROLS

Internet connectivity is no longer an option for most corporations. The information and services available are essential to the organization. This create a threat to the organization. While Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats. At the same time it is providing access to the outside world through Wide Area Networks and the Internet. Firewalls are described in subsection 5.1.1. Antivirus programs helps keeping your computer clean from harmful code, and are described in further detail in subsection 5.1.2.

5.1.1 Firewalls

The firewall is inserted between the perimises network and the Internet to establish a controlled link to act as an outer security wall or perimeter. The goal of this perimeter is to prevent Internet-based attacks. The firewall might be a single computer system or a set of several systems that cooperate to perform the firewall functionality. Firewalls are based on three basic principles of design; all traffic from inside to outside and vica versa must pass through the firewall, only authorized traffic will be allowed to pass the firewall, and the firewall itself is immune to unauthorized penetration[10].

Smith [39] lists four general techniques used by firewalls to control access and enforce the site's security policy:

- **Service control:** Determines the type of Internet services that can be accessed. The firewall filters traffic on the basis of IP addresses and TCP port numbers. It may provide proxy software that receives and interprets each service request before passing it on, or host the server software, such as Web or mail services itself.
- **Direction control:** Determines the direction in which particular service's requests may be initiated and allowed to flow through the firewall.
- **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to local users, inside the firewall perimeter. It may also be applied to external users. This however require secure authentication technology, such as provided by IPSec.
- **Behavior control:** Controls how particular services are used. The firewall may for example filter e-mail to eliminate spam.

There are several different kinds of firewalls:

- **Packet-Filtering Router:** This method applies a set of rules to each incoming and outgoing IP packet and then either forwards or discards it (see figure 5.1a). Filtering rules are based on information contained in a network packet, such as:
  - Source IP address
  - Destination IP address
  - Source and destination transport level address
  - IP protocol field

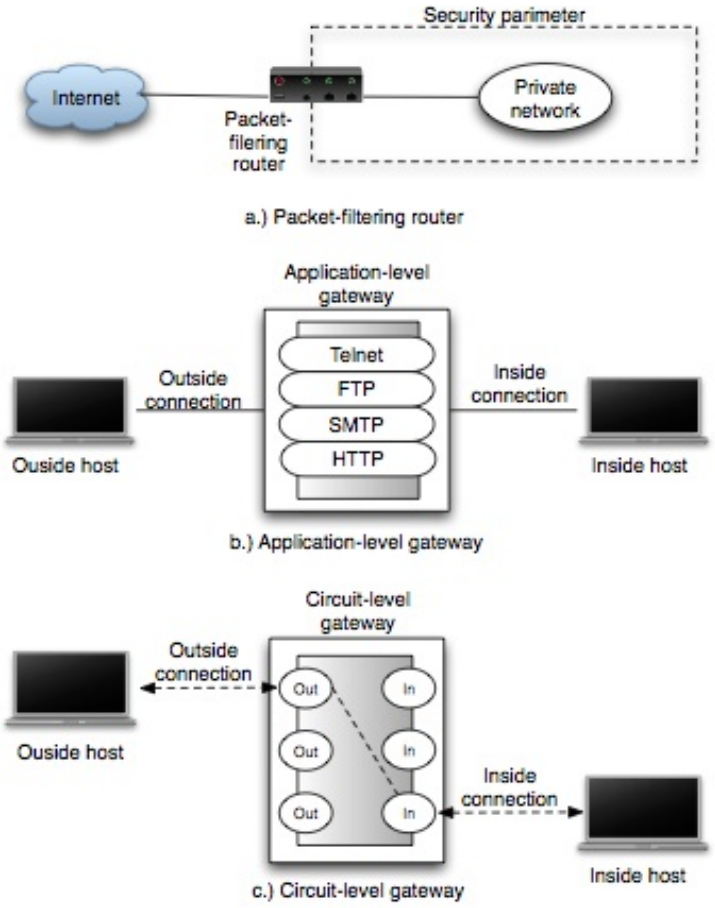

Figure 5.1: Firewall types [10]

– Interface

An advantage of the Packet-Filtering method is its simplicity. Packet filters are also often transparent to users and fast. There are however also a set of weaknesses; The filters do not examine upper-level data, bad logging functionality, no support of advanced user authentication, do not cover problems within the TCP/IP specification and protocol stack, and finally it is quite easy to accidentally configure a packet filter firewall to allow traffic types that should have been denied.

- **Stateful Inspection Firewalls:** stateful Inspection Firewalls tightens the filtering rules for TCP traffic by creating a directory of outbound TCP connections. There is an entry for each current connection, and the filter will only allow incoming traffic to higher-numbered ports for those packets fitting the profile one of the entries in the directory.
- **Application-Level Gateway:** This is also known as a Proxy Server, and acts as a relay of application-level traffic (see figure 5.1b). The user have to provide a valid user ID and authentication information to contact the wanted application. Application-Level Gateways tend to be more secure than packet filters. There are however an additional processing overhead on each connection introduced using this method.

- **Circuit-Level Gateway:** This can be a stand alone system or it can be a specialized function performed by an application-level gateway. A circuit-level gateway does not permit an end-to-end TCP connection. The gateway rather sets up two TCP connections, one between itself and a TCP user on an inner host, and one between itself and a TCP user on an outside host (see figure 5.1c). Once this connection is established, the transfers are performed without checking the content.
- **Bastion Host:** A bastion host is a system identified by the firewall administrator as a critical strong point in the network security. The bastion host typically serves as a platform for an application- or circuit-level gateway.

5.1.2 Malicious Software; Detection And Removal

Perhaps the most sophisticated types of threats to computer systems are presented by programs that exploit vulnerabilities in computing systems. These programs are called malicious programs and are a common name for a group of different threats, see figure 5.2. These threats will be presented in this subsection.

A virus is a program that can infect other programs by modifying them. The

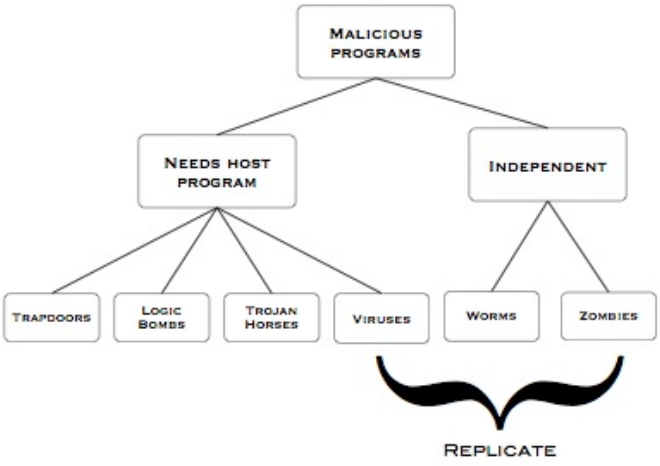

Figure 5.2: Map over different malicious software

modifications include a copy of the virus program. This code can then spread to other programs and infect these as well. A virus can be prepended or postpended to an executable program or it can be embedded in some other fashion. The key to it's operation, is that when the infected program is invoked, the virus code will be executed before the original code [10]. There are a number of different viruses:

- **Parasitic virus:** This is the most common kind of virus. It attaches itself to executable files and replicates when the infected program is executed.
- **Memory-resistant virus:** Lodges in main memory as part of a resistant system program. From that point on the virus spread to any program that executes.
- **Boot sector virus:**This kind of virus infects a boot record and spreads when the system is booted from the disk containing the virus.

- **Stealth virus:** Designed to hide itself from detection by anti virus programs. It is disguised to blend in with the original code.
- **Polymorphic virus:** Mutates with every infection, making detection by the "signature" of the virus impossible.

There are several different malwares, such as Trojan Horses, Trap Doors, Worms etc. The book "Network Security Essentials" by Stallings [10] give good descriptions on these different malicious softwares. They are also briefely described in the glossary presented in the beginning of this report.

The ideal solution to the threat of viruses is prevention. That is, not to let a virus get into the system in the first place. This goal is in general impossible to achieve. There are however some ways to limit the number of successful viral attacks. There has been a continuous arms race between virus writers and the writers of antivirus software since viruses first appeared. They provide the next best way to prevent viruses to do any harm by detecting, identifying and removing the virus from the computer system. There are four generation of antivirus software [10]:

- **First generation, simple scanners:** Requires a virus signature to identify a virus, and are limited to detecting known viruses. First generation scanners can also identify viruses by maintaining records of the length of the original programs, and reacting to changes.
- **Second generation, heuristic scanners:** These do not rely on signatures. It uses heuristic rules to search for probable virus infections, and look for fragments of code, often related to virus infections. They can also detect viruses by integrity checking by using checksums in all programs. If the checksum is altered, it is a sign of possible virus attack.
- **Third generation, activity traps:** Memory-resident programs, identifying viruses by it actions rather than its structure.
- **Fourth generation, full-featured protection:** These products are packages of a variety of different antivirus techniques used in conjunction. In addition, such a package include access control capability, which limits the ability of viruses to penetrate a system.

There are also even more sophisticated anti-virus software on the market. Two of these are:

- **Generic Decryption (GD):** GD technology enables antivirus programs to detect easily even the most complex polymorphic viruses, while maintaining fast scanning speed [40]. The polymorphic viruses decrypt itself when executed. In order to detect such a structure, the GD scanner contains the following elements:
  - CPU emulator: Software-based virtual computer that interpret the executable files instead of the underlying processor. In this way the users computer remain unaffected.
  - Virus signature scanner: Scan target code looking for known virus signatures.
  - Emulation control module: Controls the execution of the target code.

  The most difficult design issue with a GD scanner is to determine how long to run each interpretation. The longer the scanner emulates a program the more likely it catches the virus. This do however compromise the usability [10].

- **Digital Immune System:** Two major trends in Internet technology have had an increasing impact on the rate of virus propagation in recent years [41]:
  - Integrated mail systems: Systems such as Lotus Notes and Microsoft Outlook makes it very easy to send anything to anyone and to work with objects that are received.
  - Mobile-program systems: Capabilities such as Java, ActiveX and Microsoft allow programs to move on their own from one system to another.

  The Digital Immune System's objective is to provide rapid response time so that viruses can be stamped out almost as soon as they are introduced. When a new virus enters an organization, the immune system automatically captures it, analyzes it, adds detection and shielding for it, removes it, and passes information about the virus to systems running anti-virus so that it can be detected before it is allowed to run itself.

5.2 AUTHENTICATION AND IDENTIFICATION

Some knowledge about authentication protocols used in computer systems is needed to understand the underlying components used in the field of computer security. Authentication might be one way to prevent unwanted visitors on your local network or using your computers. This section provides an introduction to common protocols and their operation.

5.2.1 Kerberos

In the book Network Security Essentials [10] three threats in particular are identified:

- A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
- A user may alter the network address of a workstation so that the requests sent from the impersonating workstation appear to come from the original workstation.
- A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

The outcome of each of these scenarios is that an unauthorized users may be able to gain access to resources and data which they should not have access to. After a client and server has used Kerberos to prove their identity, they can encrypt all of their communication to assure privacy and data integrity.

One of Kerberos' key features is the *ticket service* which enables the end users to use other protected services in the network without performing log-in every time a new request is made. Kerboros enables users to communicate with other servers and entities within the same realm[1] in a single session. When a user presents a ticket to a server, the server knows the identity of the sender for sure. Precisely what this user is allowed to do is up to the server. Figure 5.3 illustrates how the authentication protocol works.

[1] A realm is the scope of a Kerberos deployment. Specifically, the organization domain for which the Key Distribution Center (KDC) is trusted to authenticate principals [10].

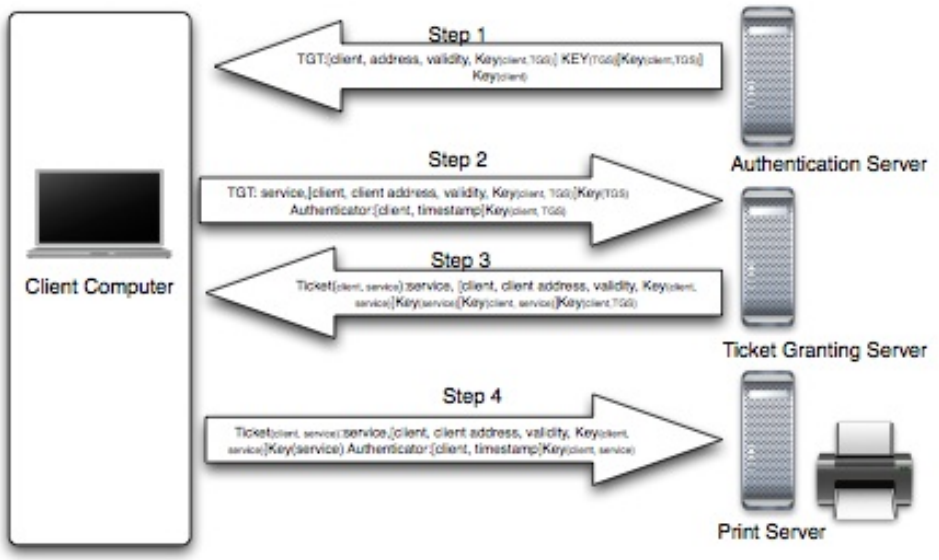

Figure 5.3: Kerberos Operation.

The client authenticates itself to the *authentication server*, then demonstrates to the *ticket granting service* that it is authorized to receive a ticket for a service. Then the client demonstrates to the *print server* that it has been approved to use the service. Kerberos is available in many commercial products including Windows 2000 [42] and Microsoft Office SharePoint Server [43], and is often used in combination with the Lightweight Directory Access Protocol (LDAP) [44], which is an open network protocol for quering and modifying directory services to form a secure directory service.

5.2.2 Action Control Lists (ACL)

The most common method of implementing access control in a computer systems is through Access Control Lists [45]. All system resources, such as files and printers have lists of authorized users. Introducing Access Control Lists enforces privilege separation. In the system, access is granted to objects based on the identity of the user and the access distribution scheme used, see section 8.2. To illustrate how this access scheme works an example is shown using NTFS[2] developed by Microsoft. This file system uses Access Control Lists to enforce security.

Figure 5.4 shows that `User1` is able to read the selected files on the partition. `User2` does not appear in the ACL, and is therefore denied access to the resource, while the entities in `Group1` have full control over the selected resource. This mechanism makes it easy for each object to check whether or not the user in question have appropriate privileges to manipulate or view it's contents.

Checking which objects a specific user of the system is able to access is very time consuming. This requires scanning all objects available on the system, and all of

[2]New Technology File System

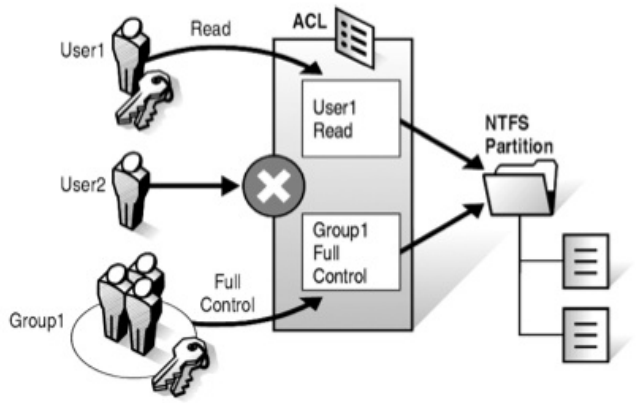

Figure 5.4: Access Control Lists exemplified by the NTFS file system [11]

their Access Control Lists. Taking into account that a system may hold millions of files, this may take days [45]. For small companies this should however not be a problem.

5.2.3 Digital Signatures

Digital signatures are used to identify the sender/owner of information. Digital signatures are created and verified by public key encryption [10, 46, 47]. The two most popular digital signature schemes are the RSA and the DSA (Digital Signature Algorithm) [48] cryptosystem which will be described later in this section. To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. The delimited information to be signed is termed the message.

The use of digital signatures usually involves two processes, one performed by

Figure 5.5: The development of signatures [12]

the signer and the other by the receiver:

- **Creating a digital signature:** A hash result are derived from the signed message and a given private key. This hash is unique to the signed message and the key used. For the hash results to be secure, there must only be a negligible possibility that the same digital signature could be created by the combination of any other message or private key.

- **Verifying a digital signature:** This process verifies the digital signature by reference to the original message and the known public key. This helpes determine whether the digital signature was created for the same message using the private key that corresponds to the referenced public key.

The security of digital signatures also depend on whether the information owner keep the private key safe or not.

Digital Signature Algorithm (DSA)

This algorithm is a *Federal Information Processing Standard (FIPS)* publication of the U.S. Department of Commerce [49]. It is the variant of the ElGamal signature mechanism [47]. The DSA was designed exclusively for signing/verification and therefore also data integrity. Other algorithms in the ElGamal family can be used for encryption/decryption and therefore key transfers, if it is necessary to use symmetric keys. The security of these algorithms are based on the difficulty of computing logarithms in a finite field. It is recommended a key length of at least 1024 bits long to provide adequate security [50].

RSA

The algorithm proposed by Ron Rivest, Adi Shamir, and Len Adleman in 1978, known as RSA, is one of the earliest and most versatile of the public key algorithms [51]. It is suited for signing/verification (and therefore data integrity), encryption/decryption, and for key establishment (key transfer). It's security is based on the difficulty of factoring very large integers. The current state of factoring research suggest use of keys at least 1024 bits long, to secure for some time to come[50].

5.3 E-MAIL FILTERING AND AUTHENTICATION

E-mail filtering is the processing of e-mail to organize it according to specific criteria. This term is often referred to as automatic processing of incoming messages, but the term also applies to the users manually removing compromised e-mails. Common uses of mail filters include removal of spam and computer viruses. There are however also possible for employers to filter outgoing messages, to ensure that employees comply with appropriate rules.

With the explosively growing reliance on electronic mail for every conceivable purpose, there is an increasing demand for authentication and confidentiality services. If an e-mail is not encrypted or signed you can never be sure that the sender's address actually represent the author of the message. Two schemes stands out as approaches that enjoy widespread use: Pretty Good Privacy (PGP) and S/MIME. These will be described briefly in subsections 5.3.2 and 5.3.3.

5.3.1 Spam-filters

The proliferation of unsolicited commercial e-mail (UCE), more commonly known as spam, over the last few years has constantly compromised the usability of e-mail. The availability of bulk mailing software and lists of e-mail addresses harvested from web pages, newsgroup archives, and service provider directories are easy. The access to this contact information allows messages to be sent blindly to millions of recipients at essentially no cost. Spam messages are extremely annoying to most

users, as they clutter their mail-boxes and prolong dial-up connections. They also waste the bandwidth and CPU time of Internet Service Providers, exposing audience to unsuitable content, and enables criminals to attempt frauds.

As of now, anti-spam filters seem to be the most viable solution to the problem. Most commercially available filters of this type currently appear to rely on simple techniques such as:

- White-lists of trusted senders
- Black-lists of known spammers
- Hand-crafted rules that block messages containing special words or phrases

On the other hand, the success of machine learning techniques in text categorization [52] has led researchers to explore learning algorithms in anti-spam filtering. Previous research work on anti-spam filtering studied the performance of many popular machine learning algorithms. Of all the existing anti-spam solutions, two classes of spam filters have emerged as the most effective and widely-deployed: Bayesian/rule-based spam filters and collaborative spam filters [53].

- **Bayesian spam filter:** A Bayesian filter uses the entire context of an e-mail in looking for words or phrases that will identify the e-mail as spam based on the experience gained from the user's sets of legitimate emails and spam [54][55]. Although the Bayesian anti-spam solutions offer very impressive performances, they suffer from two serious drawbacks [53]:
  - Bayesian filters require an initial training period and exhibit a lower performance in classifying messages composed of previously unknown words.
  - Bayesian filters are unable to block messages that do not look like a typical spam such as messages that is consist of only a URL or messages that are padded with random words.

  Recently a number of different approaches have been proposed [56][57]. They consider combining various forms of filtering with infrastructure changes, financial changes, and legal recourse to address shortcomings of regular statistical filters

- **Collaborative spam filters:** The realization of the fact that the dynamic of spam constitutes a complex phenomenon, created and distributed via the Internet, has prompted the use of collaborative spam filters. The basic idea is to use the collective memory of, and feedback from the users to reliably identify spam. That is, for every new spam that is sent out, some user must be the first one to identify it so that the rest can avoid receiving this spam by using a Bayesian filter or locally generated white and black lists. Any user that receives a suspect email can query the community of email users to find out if it has been already tagged as spam or not. In contrast to Bayesian type filters, collaborative spam filters do not suffer from the drawbacks just mentioned above, and it has been shown that they also are capable of superior spam detection performance [58, 53].

5.3.2 Pretty Good Privacy (PGP)

PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications. This report will not dive into the technologies used by the algorithms, rather give a description on how it essentially works. Deep-dives can be found in the provided citeings.

Phil Zimmerman, the creator of PGP did some essential things making PGP a good alternative for securing e-mail[10]:

1. Selected the best available cryptographic algorithms available.
2. Integrated these algorithms into a general-purpose application, independent of operating system and processor.
3. Made the whole PGP package, including the source code available online.
4. Made an agreement with a company to provide a fully compatible, low-cost version of PGP.

PGP uses a secret key paired with a public key in a public-key encryption scheme, you can learn about public-key encryption in [10] or [50]. It uses a trust model called *user-centric trust* where the main principle that each user is directly and totally responsible for deciding which certificates to trust and which to reject. In PGP a user builds or joins a so-called web of trust acting as a Certification Authority (CA) and by having his/her own public keys signed by others[50]. This is forming a network based trust model, see figure 5.6. This model might not be appropriate for

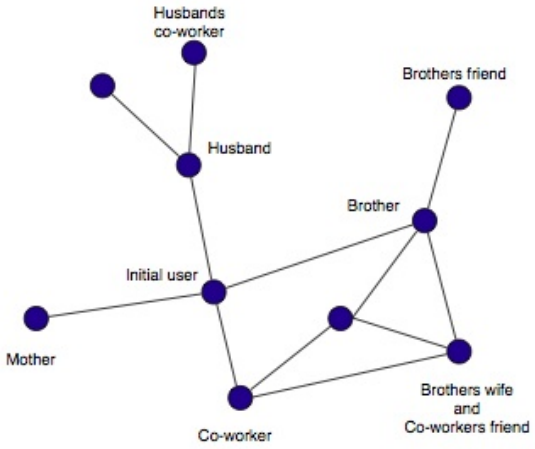

Figure 5.6: Example of user-centric trust. The initial user might based on his/her trusted network choose to accept e-mails send by someone that is trusted by someone he/she trusts.

corporate, financial, or governmental environment, since they typically want and need to exercise some control over user trust [50].

5.3.3 S/MIME

In terms of general functionality, S/MIME is very similar to PGP. Both offer the ability to sign and/or encrypt messages. S/MIME uses public-key certificates that

conform to version 3 of X.509. The key management of scheme used by S/MIME is somewhat a mix of strict X.509 certification hierarchy [50] and PGP's user-centric trust. It seems that S/MIME is the preferred method for corporations and organization due to the somewhat more structured trust management delivered by X.509.

CHAPTER 6
MOBILE THREATS

New forms of electronic communications have emerged in recent years. The mobile industry is undergoing a major change as services with new functionality such as Bluetooth, Wireless Local Area Network (WLAN), localization, music, camera, and video can be used with mobile phones and Personal Digital Assistants (PDA). Data services connection to networks such as the Internet will evolve in a greater manner in the near future. Smart Phones and PDAs will be representing the new generation of computing power[59]. The trend do however bring new challenges for information security. Threats that used to concern interconnected PCs to despite of most people unawareness now also involve the mobile workforce [13].

[59] identifies some of the most important risks in information security on mobile devices. The threats where categorized in to:

- Mobile network
- Mobile device
- Digital convergence
- Authentication threats
- Content protection

In addition I would like to mention mobile malware, which seemingly is a growing threat as smartphones becomes more and more common. Mikko Hypponen wrote an article in Scientific American, November 2006 [13] drawing a picture of how far the mobile malware has come, and the realistic future development in this area.

6.1 MOBILE MALWARE

This section describes how mobile malware develops. From Cabir, the first known mobile virus, until today's hard reality.

6.1.1 The First Strike

The first malicious software aimed at smartphones hit in 2004. It was a worm called Cabir. Cell phones have evolved into smartphones, able to download programs from the Internet and share software with each other through Bluetooth and Wi-Fi connections, worldwide multimedia messaging service (MMS) communications and memory cards these devices' capabilities have created new vulnerabilities [13]. The first virus was rather harmless, doing nothing but emptying the device's battery, while attempting to copy itself to other smartphones through a Bluetooth connection.

6.1.2 The Evolution

Although the initial version of Cabir was relatively innocent, some unscrupulous malware writers rushed to modify it into forms that are far more virulent and damaging. Other writers of such code began crafting novel kinds of attacks. A particularly aggressive form of Cabir, spread so rapidly through the audience at the 2005 world track and field championships in Helsinki that stadium operators flashed warnings on the big screen. Mobile viruses on the loose are now able to completely disable a phone, delete data or force the device to send costly messages to premium priced numbers [13]. In August 2006 more than 300 kinds of malware, among them worms, trojan horses, viruses and spyware, were known to be unleashed against devices, see figure 6.1.

Multiple new functionalites in mobile phones has given a new generation mobile

Figure 6.1: Growth in mobile malware [13]

phones called smart phones. These consist of the functionalities that is described in the preface of this chapter. Each of these features offer a conduit through which malware can propagate. Bluetooth, for example, allows certain mobile worms to spread among vulnerable phones by mere proximity, almost like the influenza virus [13]. Most smartphones can put Bluetooth into a “nondiscoverable” mode that protects them from invasion by worms. But few users are familiar with this feature [13].

While giving a speech at the security conference, Hoppinen performed a quick scan of the audience to find out how many had left their Bluetooth on. Nearly half of the professionals in the audience did actually keep the Bluetooth wide open. Hoppinen predict that the numbers are even worse among the regular population. Many of the smartphone users do not even know the feature is there, and certainly not how to turn it off.

The attacks are getting constantly more evil every day. Increase in theft of financial data, business secrets or computer resources illustrates that the motivation of these crimes has turned from mere mischief actions to crimes with intention of pure profit.

6.1.3 A Mobile Attack Scenario

This scenario is gathered from Happinens article on Mobile Malware, [13]. CommWarior is a mobile worm, that are known in about 15 variants. CommWarrior exploits the Bluetooth interface to populate onto new devices. It persuades victims to accept the malware onto their phones using denial of service methods until the victim gives in. Here is a scenario on how malware typically would operate:

1. One day on the Bus, Bob's smart phone beeps. Another device in the bus is carrying CommWarior.Q which is trying to copy itself onto Bob's smart phone via Bluetooth.
2. Bob's phone alerts him that someone is trying to send him a file, and asks him to accept or decline this attempt.
3. Bob gets suspicious and of course declines this request. The phone however keep beeping, presenting the same request over and over. Bob can not do anything with his phone at this point.
4. Suddenly Bob needs to make an urgent phone call, and has no other choice than accept the continuous attempts of the file transfer. If Bob now tries to insert his memory card into another phone, this phone would get infected as well.
5. CommWarior.Q starts scanning for new Bluetooth devices, and tries to copy itself onto the ones it finds.
6. Bob sends Alice a text message. The worm immediately sends Alice a follow up MMS file containing a copy of the worm. The file has a plausible file name. When Alice opens the message, her phone gets infected.
7. The worm now sends MMS copies of itself to the complete phonebook registry on Alice's phone, along with a text message assembled from Alice's past messages.
8. Every time Alice replies to a text message, CommWarior.Q sends a follow up MMS package. Alice's carrier charges for every MMS message she sends, so her bill becomes quite a surprise at the end of the month.

This scenario shows how a virus might appear and lure users to open infected files. Even professional users, might fall into these traps.

6.1.4 The Future

Hopefully the lessons learned in the development of malware distribution in regular PC's will help anticipating what steps the mobile malware writers will take next, and be prepared when they strike. We are however enormously far from in control at the moment, and it is hard to say if the mobile malware will strike harder than it did for the population of PC's. Some of the efforts that might prevent viruses are [13]:

- Carriers would be wise to begin educating cellular customers now about how to identify and avoid mobile viruses.
- Phone makers should install antivirus software by default.

- Regulators and phone companies can also help avoid the monoculture problem that plagues PCs by encouraging a diverse ecosystem for smartphones in which no single variety of software dominates the market.

6.2 MOBILE NETWORK THREATS

The most concrete threats against mobile networks may be the eavesdropping on phone calls and data traffic, similar to the threats experienced with data transfer between PCs. Use of encryption makes it more difficult to succeed in this. The probability of this threat depends on the strength of the encryption algorithm. This strength has turned out to be questionable in the GSM(Global System for Mobile communication) network [46]. A more hypothetical, yet scarier threat, is altering the original mobile traffic into something else. The intruders then might replace the original traffic with their own. In these attacks the intruders exploitation scenarios are limited, the most beneficial information would for instance be location information and user profile information.

Another threat on mobile networks are the Denial of Service (DoS) attack. This might be a very serious threat, if you take emergency communications into account. This might however lead to decrease in productivity and loss of time and money for companies. Mobile devices are typically vulnerable to these attack due to the need for trusting the available network service operator on whatever location you are. In case of forged base stations, the users might be really easy targets. The best known vulnerabilities in GSM are listed in table 6.1. In UMTS (Universal Mobile Telecommunications Service) however these shortcomings seems to be fixed in great extent. DoS attack are however also possible in this third generation mobile technology.

Threat type	Threat
Authentication	The user does not recognize a forged base station
Authentication	Same identity codes can be present in multiple devices after production
Authentication	Weak authentication algorithms
Confidentiality	Keys and authentication information are to encrypted in the operators fixed network
Confidentiality	Weak encryption algorithms
Integrity	Data integrity is not checked
User guidance	The user cannot see whether encryption is used or not
Maintenance	Inflexibility. It is difficult to update security functions

Table 6.1: Shortcomings in the GSM network [59]

6.3 MOBILE DEVICE THREATS

The main threat to the mobile devices is stealing and tampering, due to its small size and great portability[59]. There might be catastrophic outcomes if mobile devices are stolen, since mobile phones now have become an important content manager in professional businesses. The fact that only 11% of Norwegian companies are encrypting their portable equipment [28], make the risk explode. There are multiple examples of personal content distributed on web, media and other channels after the loss off portable equipment, such as mobile phones. This illustrates how easy it is to forget that information once on personal devices, no longer are personal or

confidential if the devices are lost.

New mobile phone models have an increased likelihood of getting virus infections due to the use of general purpose programming languages such as Java [59]. These might for instance be distributed by compromised SMS (Short Message Service) messages, MMS (Multimedia Messaging System) messages, WAP (Wireless Application Protocol) pages, internet pages and rapidly streaming malware. The threats include the ones already familiar in the internet world, such as trojan horses, worms, key loggers and spyware.

There has been a lot of discussion about information security issues in Bluetooth [60] devices. The threats concerning Bluetooth to great extent also apply to Wi-Fi[61] and other similar technologies as well. Perhaps the most significant source of risks in wireless connectivity is that the technology's underlying communications medium, the airwave is open to intruders. Bluetooth has three different modes of security. Each Bluetooth device can operate in only one mode at a particular time. The three modes are the following [60]:

- *Non-secure mode*: In this security mode (Mode 1) the device will not initiate any security procedures. A Bluetooth device in security mode 1 is in a promiscuous mode that allows other Bluetooth devices to connect to it.

- *Service-level enforced security mode*: In this mode, the notion of authorization, that is the process of deciding if device A is allowed to have access to service X is introduced. Security procedures are initiated after channel establishment at the Logical Link Control and Adaption Protocol (L2CAP) level[62]. For this security mode, a security manager controls access to services and to devices. The centralized security manager maintains polices for access control and interfaces with other protocols and device users. Varying security polices and trust levels to restrict access may be defined for applications with different security requirements operating in parallel. Therefore, it is possible to grant access to some services without providing access to other services.

- *Link-level enforced security mode*: In the link-level security mode, a Bluetooth device initiates security procedures before the channel is established. This is a built-in security mechanism, and it is not aware of any application layer security that may exist. This mode supports authentication and encryption. These features are based on a secret link key that is shared by a pair of devices. To generate this key, a pairing procedure is used when the two devices communicate for the first time. Two associated devices simultaneously derive link keys during the initialization phase when a user enters an identical PIN into both devices. The PIN entry, device association, and key derivation are depicted conceptually in Figure 6.2.

6.4 Threats Due to Digital Convergence

Because of the digital convergence, the complexity and number of interfaces in devices is increasing. This in terms lead to an increased need for management of the system as a whole. One cannot assume that input to mobile devices are harmless. The reliability of the software becomes more and more critical, as well as its ability to filter out deficient data from it's surroundings. The use of broadcasting techniques in service production also increase the number of service threat scenarios (e.g. in denial of service or authentication threats).

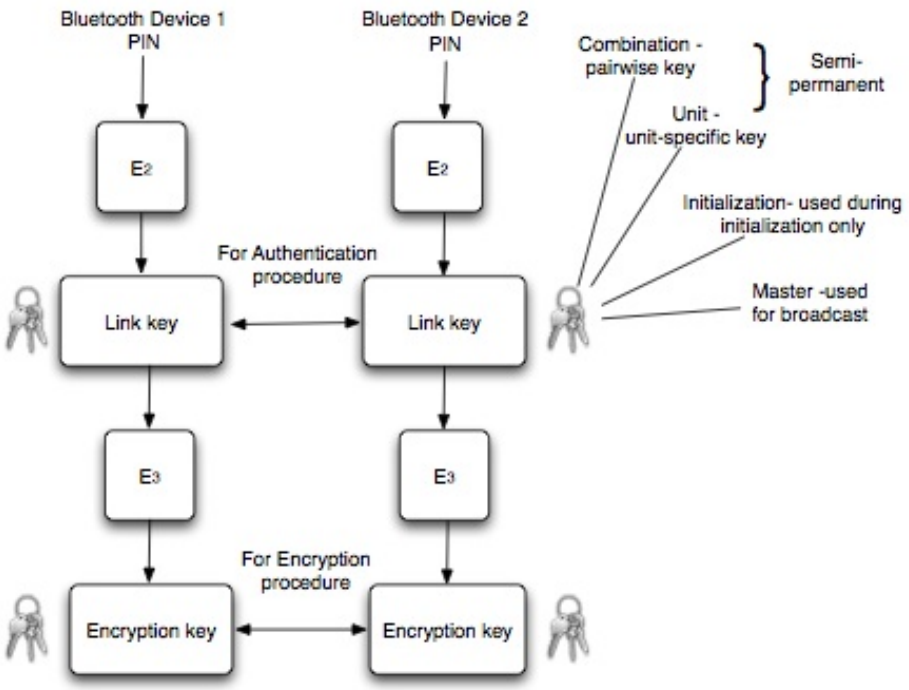

Figure 6.2: Bluetooth key generation from PIN [14]

One serious threat is the possibility of attack on the software in mobile devices using any network connection. If this type of attack was successful, attacks against the Internet and payment services would be a possible threat to Internet devices [59].

6.5 Threats to Authentication

These kinds of threats may be divided into two groups:

- Threats connected to user and mobile device's authentication carried out by the network.
- Threats connected to the networks authentication by the user and the mobile device

The major authentication threats for the service developer are forged or illegally commissioned mobile devices. Authentication is based on cryptographic authentication algorithms. A weak algorithm generates a threat, enabling disclosure and copying of the secret key stored in the SIM(Subscriber Identity Module) card. As a consequence, use of certified mobile services without a SIM card becomes possible if the secret key are stolen, either separately or with the mobile device.

Additionally there are the *"Man in the middle attacks"*, in which the session initiated by the user is seized by a hostile user. This is not a new unique method of attack for the mobile industry, but their implementation is more troublesome in the air interface, compared to the fixed networks. The reasons for these attacks are

rarely technical. Even though one major flaw in authentication algorithm might be the reason why data are incriminated, the information security awareness of the users are the most important measure to avoid them. I will describe security awareness in detail in chapter 7.

6.6 Content Protection Issues

The biggest concern for content protection is piracy. Content protection is a new field for which standardized and definitively good solutions are not yet available[59]. Content protection issues can even restrict or prevent the supply of certain services. The upcoming features, available for instance in the Office 2007 suite and Exchange mail server where content might be downloaded and processed directly on the mobile devices create concerns. It seems to be very difficult for the users to realize the differences between professional and personal use of the device. This despite the fact that differentiated protection has been executed on stationary PC's for quite some time.

CHAPTER 7
SECURITY AWARENESS

[28] states that only 40% of businesses have had training for their employees in secure use of information technology. The fact that most companies actually spends money on technical assurances against information crime, but at the same time do not see the dangers in incompetent employees using this technology is frightening. Based on statistics from SSB [1] it is estimated that Norwegian businesses in total were victims of about 3900 data intrutions the last 12 months. In the cases where the intruders were identified, nearly half were employees or hired help in the companies at stake. However, only 61 cases of data break-ins where reported in the same period. In the same manner there were an estimated 8900 cases of ICT-resource abuse, but only 11 reports filed.

These frightening numbers indicates the desperates need for action in educating and providing awareness of information security in companies. In section 7.1i will look at educational possibilities for companies and in section 7.2 look at the attitudes employees have towards security and possible actions to improve these attitudes. Section **??** will describe why it is so important to secure your information in all the steps of a process.

7.1 EDUCATING THE EMPLOYEES

Mariana Hentea [63] proposes that information security is something one has to grow up with to be able to handle properly:

> "It is becoming obvious that information security awareness has to be provided to students at an earlier age. If we teach children security awareness earlier, they will be prepared to pay attention to security matters as well as to avoid getting engaged in illegal behavior. In addition, education on information security awareness must be provided to teachers and parents. These are the most important people in the youngsters' lives. If we teach educators and parents how to handle information security issues and how to use computers, they will be better prepared to provide training to youngsters."

Although this probably is true, and in time will improve the general information security awareness, I also believe it is important for employers to have proper learning programs for their employees to gain as much knowledge as possible about these issues.

[1] Statistisk sentralbyråURL: www.ssb.no

7.1.1 Common Knowledge

Security awareness is one of the most effective security methods of the information security assurance. However statistics indicate that the problem of low information security awareness is not resolved in all US organizations. This is because many ICT users lack the basic security training and organizations do not have budgets or strategies in place for training [64].

The article [8] describes a study performed on home-based small businesses in 2006. A survey was sent to 800 companies, and there were 232 complete answers. The data was processed and analyzed using [65]. The first question addressed the extent to which home-based small business owners are aware of the increased threats facing their businesses because their computer system is connected to the Internet. The most knowledgeable categories were:

- Spam e-mail
- Virus attacks
- Pop-ups

The highest unaware categories where:

- Trojan horse
- Spyware

The study concluded that small business owners are well aware of the problem with more attacks, yet less than half of them are proactively taking appropriate measures to adequately protect their computer systems. This is probably due to lack of knowledge of how much damage an attack can do to the productivity and reliability of a company, see section 4.4. The calculations of this are described to more extent in chapter 9.

7.1.2 Simulation Teaching Tools

Education and training in computer security is often mundane and boring for both users and administrators [15]. There is a considerable amount of useful information published about the fundamental concepts of computer security [66, 67, 68], but sometimes people have to experience the problem in order to understand it [15]. There are also a number of information security training providers in Norway. Some of these are:

- NorSIS
- nettvett.no
- Masterminds
- DataEquipment
- saftonline.no (for children)
- KITH (Health and social sector)
- Datasikkerhet.net

In companies where there are ICT-specialists, they can probably hold courses on security internally.

Since the common knowledge do not seem to be the main problem, I choose to take a better look at more innovative educating alternatives, such as simulation teaching tools. Center for the Information Systems Studies and Research (CISR) at the Naval Postgraduate School, located in Monterey, California[2] have developed such a tool sponsored by US Navy, the Naval Education and Training Command, the Office of Naval Research, and the Office of the Secretary of Defense. The name of this game is CyberCIEGE^{TM}.

CyberCIEGE^{TM} [69, 15, 70] enhances information assurance education and training through the use of computer gaming techniques such as those employed in SimCity^{TM} and RollerCoaster Tycoon®. In the CyberCIEGE^{TM} virtual world, users spend virtual money to operate and defend their networks, and can watch the consequences of their choices while under attack. The player of the game constructs computer networks and makes choices affecting the ability of these networks and the game's virtual users to protect valuable assets from attack by both vandals and well motivated professionals. The game introduces the player to the need for well formed information security policies, allowing the player to deploy a variety of means to enforce security policies, including authentication, audit and access controls. The game will depict a number of vulnerabilities ranging from trivial passwords to trap doors planted by highly skilled, well-funded adversaries.

The effectiveness of CyberCIEGE^{TM} for basic information assurance awareness

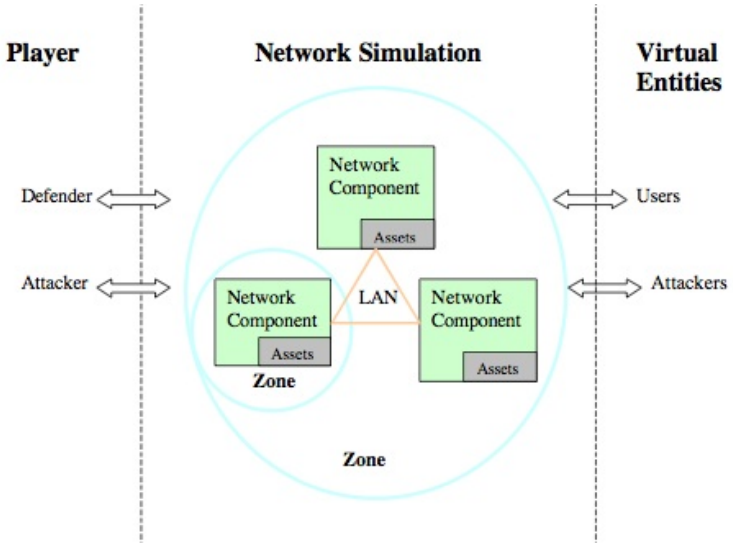

Figure 7.1: An overview illustration of the relationship between the network simulation and other game elements[15].

has not yet been fully assessed. While initial feedback has been positive, a side-by-side comparison with traditional on-line click-through awareness programs (DoD, 2006) is needed. Some experiences with CyperCIEGE^{TM} show that there are users

[2]"CISR is America's foremost center for defense-related research and education in Information Assurance (IA), Inherently Trustworthy Systems (ITC), and defensive information warfare." http://cisr.nps.navy.mil/

that simply will not expend any effort to learn even the most basic mechanics of a video game. For these users, interactive training methods will not be effective if they require anything more than repeated clicking of a mouse or pressing a key. We are however traveling at high velocity into the digital age, where the new generations are far more forthcoming to new technology. This make me believe CyberCIEGE^{TM} and similar teaching tools might become valuable in the close future.

7.2 POSTURAL WORK

Earlier this year I received an e-mail from the ICT-director at my company. She wanted to introduce a new policy regarding passwords to log on to our ICT-systems. Earlier it was possible to keep the same password for as long as you wanted, now you have to change every 90 days. When you change your password, the new one has to be different from the 10 most recently used ones. I looked around in the office and noticed that the highly trained ICT consultants where all nagging about this new policy. Within ten minutes after I had received the ICT-directors e-mail there were four more e-mails in my inbox. These were from colleagues sharing their thoughts and rather innovative suggestions on how these new policies could be avoided or how to "fool" the system. This caused me to detect that the laziness might also be one of the most important factors in securing the information despite of the companies own employees. This also indicates need for explanations on why this policy is activated, and which threats this address.

In this section I will consider some of the most common risks taken by employees when it comes to compromising the information security of their company. These common "mistakes" are well known security traps, that most likely are listed in the companies ICT-policy if such exists. In my experience the employees are ignoring the policy and knowledge due to several different reasons, such as:

- "It won't happened to me"-attitude
- Laziness
- Distractions
- Simply forgetting to follow best-practices
- Do not know what the policy is protecting against

7.2.1 Passwords

I believe the scenario described in the beginning of this section unfortunately is quite common for businesses. There are also other common traps when it comes to authentication and passwords:

- Choosing a trivial password
- Using the "remember me"-option when logging onto systems
- Using identical password on multiple systems
- Keeping a password for too long
- Not keeping the password private

- Writing the password down instead of remembering it

This is probably the easiest way into a system for intruders. Obtaining a password and username is not hard. It is important to avoid these traps to limit the possibilities for the attacker, and limit the loss if some authentication credentials are compromised.

7.2.2 Lock Computer When Leaving Workstation

There are many offices and workstations that are easily accessed for others than the owner. People tend to forget that even though you work at a facility where you need a key to get in, colleagues might be just as big of a threat as people from the outside. Leaving for a short break or a trip to the coffee machine might be enough to access and abuse valuable information. Locking the computer is easy to do, but also easy to forget. Taking actions to get employees to use this extremely easy feature might be worth a lot. This is not about education. Most people know that this is an option, and that it is best-practice to use it. Some actions to make people use this feature is:

- If you work in an open office environment, it might be a smart solution to make employees check up on their co-workers. Make it the whole departments responsibility that all computers are locked when not in use.
- To limit danger if forgotten to lock workstation, there might be useful to use automatic lock. This might be timed as desired. It is important to find a good timer value, to short will become annoying and too long might not be of value at all.
- Or a more humerous approach; encourage employees to change the background picture of any unlocked computer to something else, or change the language to something not understandable to the computer owner.

7.2.3 Do Not Let Equipment Out Of Sight When Traveling

If you have just arrived at your destination and want to grab a bite before checking into your hotel, it is common to meet luggage-restrictions at the restaurants. “Please leave your bag with us while eating” is a line you often get to hear if you try to bring the bag in with you. There are however numerous examples of laptops and other equipment disappearing at these depots. But is it really safe to keep it at your hotel room while eating instead? Probably not.

Another place where equipment seem to disappear is during transportation. Taxies are a common place to forget belongings. It is rather difficult to get the hold of the taxi you used if you do not have the receipt or remember the taxi-number. There are a lot of examples of belongings forgotten in cabs that are not returned to the owner or reported found to the taxi-company. In which cases would the loss be covered, and which should the employees be held responsible for?

7.2.4 Installing Updates And Security Patches

Trying to keep up with the malicious intruders in the computing industry, application providers such as Microsoft, Apple, Mozilla, Norton Anti Virus and others

are continuously improving their applications. These improvements are often distributed as security updates or security patches. To obtain the highest level of protection it is important to install these released updates properly, immediately after release.

Most operation systems do have functionality to automatically check for updates of your installed software online. You are able to personalize this functionality by customizing checking intervals. For Microsoft this functionality is called Automatic Update and can to be found in the Security Center at the Control Panel. When turning on Automatic Updates, Windows routinely checks the Windows Update Web site for high-priority updates that can help protect the computer from latest viruses and other security threats [71]. These updates can include security updates, critical updates, and service packs. Depending on the settings you choose, Windows automatically downloads and installs any high-priority updates that the computer needs, or notifies the user as these updates become available. Windows automatic updates also provide options for system administrators to lock this functionality, so that the user can not turn the functionality off. Mac OS-X and Linux also provide similar functionality.

7.2.5 Suspicious E-mails And Malicious Web-sites

As scam artists become more sophisticated, so do their phising e-mail and pop-up windows. They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web Sites. This makes the scam attempt harder to detect. There are however some key elements that should make the users suspicious:

- "Verify you account": Legitime businesses will not ask you to send passwords, login names, Social Security numbers, or other personal and sensitive information through e-mail.
- "If you don't respond within 48 hours, your account will be closed": These messages convey a sense of urgency so that you will respond immediately, without considering if it is a scam or not.
- "Dear Valued Customer": Phishing e-mails are often sent out in bulks and do not contain any personal information about you, not even your name.
- "Click the link below to gain access to your account": HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site. The links that you are urged to click may contain all or part of a real company's name and are usually "masked," meaning that the link you see does not take you to that address but somewhere different, usually a phony Web site. By hovering the mouse over the link, you can reveal the real link, and detect the scam, se figure 7.2.

To help protect from these incidents besides using common sense, there are phishing filters available for download. These are free of charge or automatically installed on the browser.

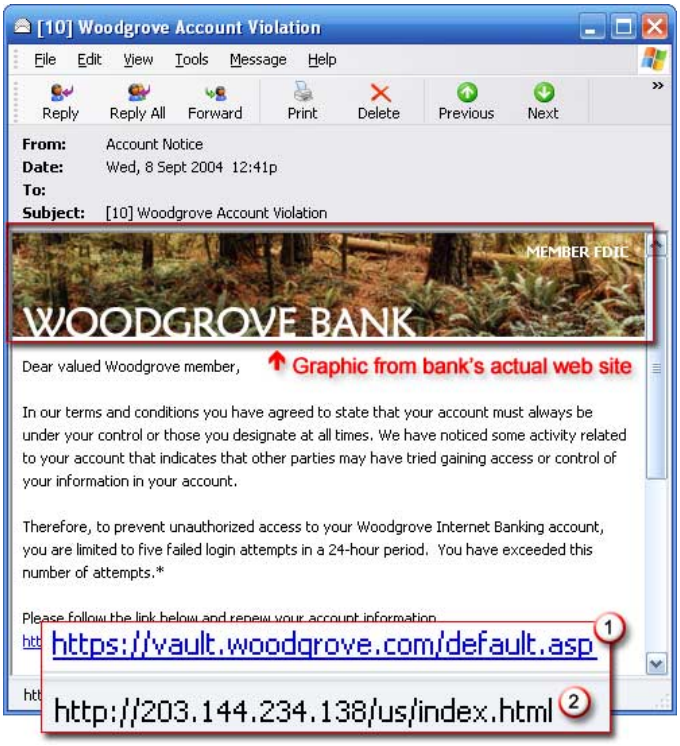

Figure 7.2: Example of a phishing e-mail, including a deceptive URL address linking to a scam Web Site [16].

CHAPTER 8
SECURITY MANAGEMENT

The words

> ”Know the enemy, and know yourself, and in a hundred battles you will never be in peril”

spoken by the Chinese general Sun Tzu over 2500 years ago, still remains valid for the battle of information security for today's companies. Knowing the enemy faced by information security is a vital component to shaping an information security defense posture. None the less, the importance of knowing our own vulnerabilities in the battle against malicious intruders or simply employees unawareness are critical. There are numerous threats and small companies can never be secured against all of these due to the large costs. In Figure 8.1 you se a number of different information security threats. The key to securing your information are to identify the ones important to you and initiate action for protection, the key term here are risk management, which will be discussed in section 8.3.

It is also important for managers to delegate the right access to information to

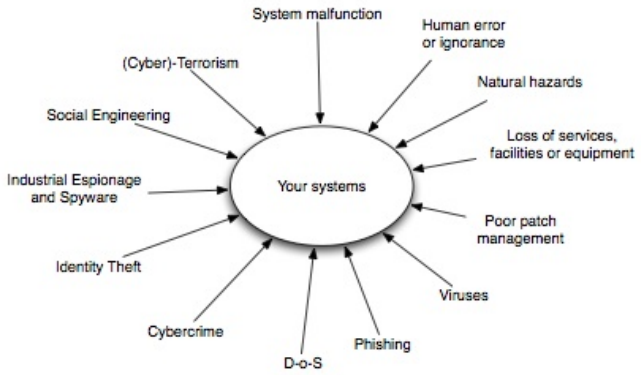

Figure 8.1: Threats to consider when securing your information

the right people and to know how to handle possible threats before they appear, and after. This might be done by using standards for handling information security breaches. The sections 8.2 and 8.1 will discuss these matters. In most cases small companies do not have the necessary skills to manage ICT and information security in-house. These have the choice of outsourcing the ICT and information security services of the company. This option are presented in section 8.4.

8.1 INFORMATION SECURITY STANDARDS

Information security standards provide a framework from which to develop information security policies, practices and procedures tailored to an organizations risk requirements. It is important for managers to find and use the standards appropriate for their organizations. Results from the Australian Computer Crime Surveys [3, 4] indicates that the use of such standards are a cruitial method in fighting computer crime. Standards most often used to be country specific, however this section present some of the most used international standards. Common Criteria will be described more closely in subsection **??**, since this is the resulting standard from several national security standard initiatives.

8.1.1 ISO/IEC Standards

ISO is short for International Organization for standardization and IEC for International Electrotechnical Commission. They provide multiple standards for information security. Some of these are:

- **ISO/IEC 27001:** Specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks [72].
- **ISO/IEC 17799:** Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization [72].
- **ISO/IEC 13335:** Concepts and models for information and communications technology security management [72].
- **ISO/IEC 15408:** Common Criteria [73] standard.

8.1.2 Common Criteria

With the rise of security breaches and the running of technology at its highest gear on the information highway, protection of confidential and vital information never has been more crucial. The "Orange Book" - TCSEC in the US 1985, started the needs to have some assurance that the products and the systems used, provides an adequate security. After this, various countries began their initiatives to develop evaluation criterias that builds up on the concept of TCSEC; in Europe - ITSEC(1991), Canada -CTCPEC(1993), US - Federal Criteria. The Common Criteria - ISO/IEC 15408 - Evaluation Criteria for Information Technology Security represents the outcome of series of efforts to develop criterias for evaluation of ICT security[73].

Unlike most other standards, Common Criteria does not provide a list of product security requirements products must contain. Instead, it describes a framework in which computer system users can specify their security requirements. Vendors can then implement and/or make claims about the security attributes of their products. Testing laboratories then evaluate the products to determine if they actually meet these claims. Common Criteria attempts to provide assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a dependable and standard manner.

Creation of the Protection Profile (PP)

The Common Criteria (CC) for Information Technology Security Evaluation [74] defines that a Protection Profile (PP) should be developed for a specific Target of Evaluation (TOE). The creation of a PP follow three stages after it's introductory definition, shown in figure 8.2 The purpose of the protection profile is to state a

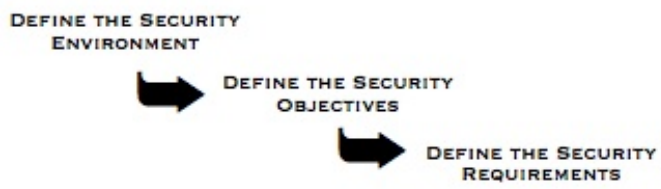

Figure 8.2: Developing a Protection Profile, the three stages [17].

security problem for a given set of systems, known as the target of evaluation (TOE), and to specify security requirements to address the problem without dictating how these requirements should be implemented [75].

The Security Target

In response to the defined PP a Security Target (ST) is made. A ST is a combination of security objectives, functional and assurance requirements, summary specifications, PP claims, and rationales [75]. In other words ST presents a detailed design architecture for the system security. An approved ST is used by developers to produce the TOE.

Security Assurance Activities

Security assurance provides confidence that a product or system will meet, has met, and is continuing to meet its stated security objectives [73]. Security assurance activities should not be a one time test, but a continuous workload through all stages in a project, including maintenance [75].

8.2 Access Control and Access Distribution

An access control system enforces a policy on who may access what resources and in what manner on a system [76]. This chapter will cover some common access schemes frequently used in systems on the marked today. These describe different ways to delegate access privileges to employees. A short explanation on how these work and their use is described to give an introduction on how they can be implemented to secure information. It is important for managers to select the best fitted access control scheme for thir organization to protect information at the lowest cost possible.

8.2.1 The Principle of Least Privilege

The principle of least privilege is an old administrative practice of assigning permissions to users which holds that each principal should be accorded the minimum

access needed to accomplish it's tasks [77]. This avoids the problem of users having the ability to perform unnecessary, unwanted or harmful actions. Clearly, richer notions of "minimum access" allow the principle of least privilege to discriminate better between those actions that should and those that should not be allowed. An administrator may want to have the powers of a normal user most of the time, and exercise his extraordinary powers only when needed. It is important that an untrusted person should not be able to increase its powers beyond those granted initially.

Figure 8.3a illustrates a simplified scenario on how the principle of least privi-

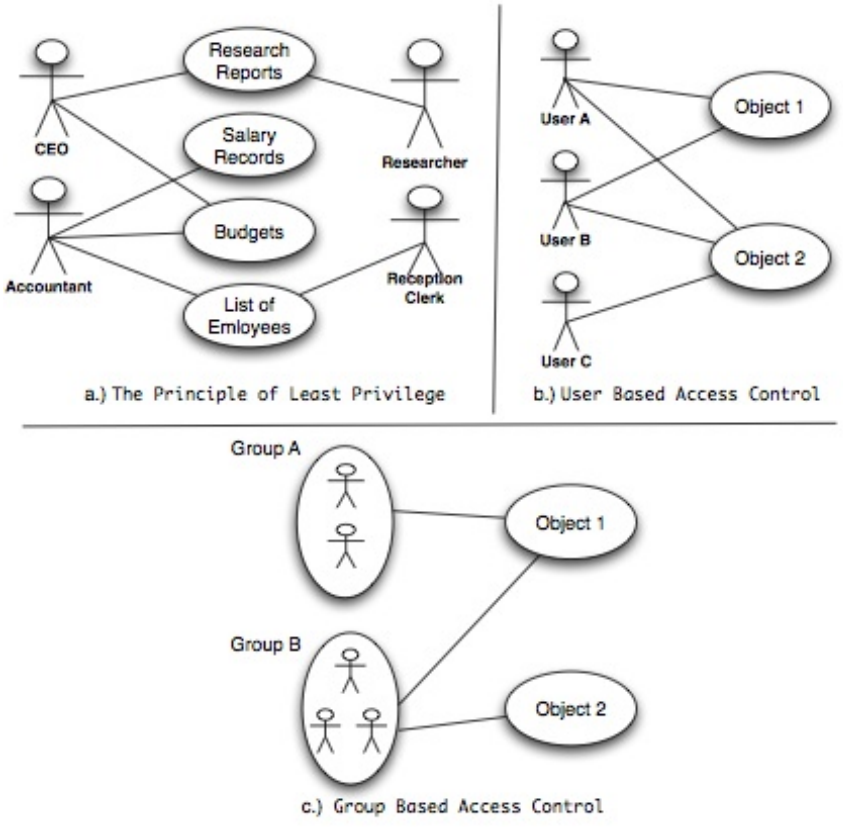

Figure 8.3: a.)The principle of least privilege applied to a typical small business environment. b.) Example of User Based Access Distribution. c.) Example of Group Based Access Distribution

lege may be implemented in a small research environment. The researcher needs access to research reports, but the reception clerk does not and is therefore not able to access them. The clerk at the front desk needs access to the complete list of employees at the institution, and so does the people dealing with accounting. They will therefore be granted access to these. The accounting person also needs access to the employee's salaries and budgets to be able to manage payment and economical planning. The CEO will normally have access to all company information but he does not need information to anything but research reports to se how the company is doing and the budgets for planning. He will however be able to ask for additional access when needed and be granted this information. There will probably not be as

easy for the reception clerk to be granted access to research reports.

8.2.2 User Based Access Control

The notion of user identity is probably the most pervasive concept in access control modeling. When access based on user accounts is prefered, permissions is given directly to each user. Each user has a distinct set of permissions. Access based on user accounts are easy to make, but can be very complex to maintain in large systems [78].

Figure 8.3b illustrates how the user based access control authorization maps each subject into an equivalence class based on their user attributes. Based on these equivalence classes and the object identity, permission to system resources are granted [79]. This results in a higher workload for the administrators of the system. If all normal users have access to a new program, the administrator has to add each user to the program's access list. In small companies this should not be a big job. Most companies probably wishes to expand at some point, this can lead to scaling problems.

8.2.3 Group Based Access Control

In group based access control, users are organized into different groups [80]. Figure 8.3c illustrates how a user inherits all the privileges of the groups he is a member of. This makes maintenance of user privileges easier than for user based access, since an administrator can change the access rights of multiple users by changing the privileges of the groups they belong to.

Access permissions on documents and other relevant parts of the system are granted to user groups for specific operations. User groups can be used to model roles by, for instance assigning a job function name to a group and defining many subgroups for various tasks [80].

8.2.4 Role Based Access Control (RBAC)

The concept of RBAC is relatively simple and is quite similar to the group based access control discussed in section 8.2.3. Access to different parts of a computer system is based on a user's role in the organization.

Simple forms of handling access this way dates back to the 1970s, when implementations were made in business organizations and commercial computer applications [45]. Today RBAC is a widespread and well known concept. A role exists as a structure separate from the one describing the user. The different roles should adhere the principle of least privilege in which a role is created with minimum permissions in specification of duty requirements as described in 8.2.1. The basic concept of RBAC is that users are assigned to roles, permissions are assigned to roles and users acquire permissions by being members of roles [45].

The core RBAC model relations are defined in figure 8.4 as a part of the proposed standard [18] by Ferraiolo et al. The core includes sets of five basic data elements

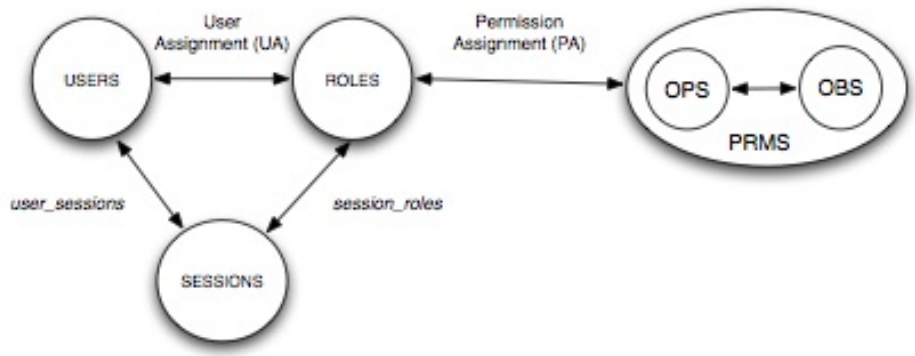

Figure 8.4: The core of the RBAC model [18]

called users (USERS), roles (ROLES), objects (OBS), operations (OPS) and permissions (PRMS). The model as a whole is fundamentally defined in terms of individual users and permissions being assigned to roles. These roles can be presented in role hierarchies.

Role Hierarchies

There are three primary kinds of role hierarchies which might exist in an organization [81].

- The *isa* role hierarchy, based on generalization.
- The *activity* role hierarchy, based on aggregation.
- The *supervision* role hierarchy, based on the organizational hierarchy of positions.

Figure 8.5 gives an example of a hierarchy consisting of health care personnel. The `Physician` role is superior to `Health-care provider` and inherits all of this role's permissions. The `Physician` role can have permissions in addition to those inherited from the `Health-care provider` role. Inheritance of permissions is transitive so, the `Primary-care physician` role inherits permissions from the `Physician` and `Health-care provider` roles. `Primary-care physician` and `Specialist physician` both inherit permissions from the `Physician` role, but each of these will have different permissions directly assigned to it.

It is possible to assign multiple roles to an identity, and have the same user assigned to multiple roles. The roles might also be assigned multiple permissions. The users can exercise the permissions of multiple roles at the same time. Time limited access is also a feature in RBAC. It is possible to restrict the roles to have some permissions only for a limited period of time. One example where this might be useful would be if a doctor's neighbor is admitted to a hospital at this doctor's department. If the doctor is not the one responsible for treating the neighbor, this special relation should prohibit the doctor from looking at the patient's medical record [30].

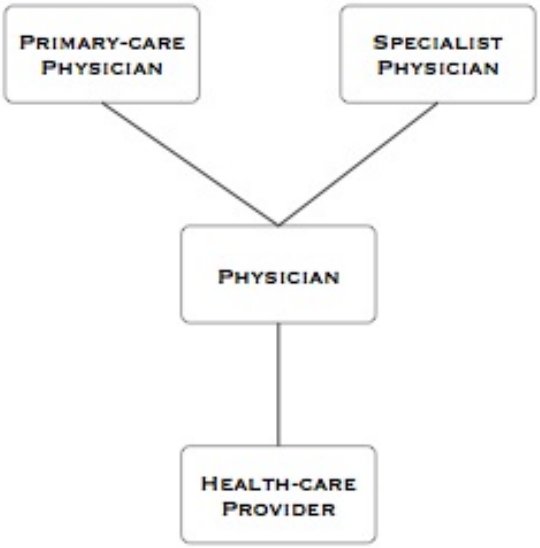

Figure 8.5: RBAC hierarchies [19]

8.3 MANAGING RISK

Businesses routinely manage risk as part of their day-to-day operations. Risks can be measured using a variety of mechanisms described in this section, including:

- Indemnification
- Mitigation
- Retention
- Liability transfer

It is crucial for businesses to be able to manage and understand their own risk, for the purpose of making decisions on how information security should be handled.

8.3.1 Liability Transfer

A business can transfer liability for an adverse event to another party. This takes the risk away from the business' and over to a third party in one of two possible ways [37]:

- **By disclaimer:** A business disclaims liability by undertaking an activity with the explicit understanding that it will not be held responsible for the consequences of certain adverse events. This is done without specifying who will be responsible for those consequences.
- **By agreement:** A business transfers liability by entering into an agreement with a counterparty. The business engages in an activity with a counterparty only after they both agree that the counterparty will be responsible for the consequences of certain adverse events.

8.3.2 Indemnification

Indemnifying can be defined as:

> "Agree to compensate for damage or loss. The word is used in insurance policies promising that, in the event of a loss, the insured will be restored to the financial position that existed prior to the loss."[1]

There are two major types of indemnification [37]:

- **Pooling:** Several businesses share the cost of certain risks. You typically find this in insurance policies. If an adverse event is unlikely to happen at the same time to a meaningful fraction of the pool, pooling will decrease the cost of risk for each business in the pool.
- **Hedging:** A single business places a bet that an adverse event will happen to it. If the event is not likely to take place, other companies most likely will be willing to take the bet. If the event do not occur, the bet placer have to pay the betters, but if the event do occur the betters have to pay their part of the losses experienced due to the adverse event.

8.3.3 Mitigation

A business can try to reduce the expected cost of risk, either by reducing the probability of an adverse event occurring, or reducing the consequences if it does. This is probably a more common sence risk management tactic, requiring implementation of security measures described in chapters 5, 6 and 7.

- **Reducing probability of adverse event:** This can be done by redesigning systems or processes to eliminate the known event's or suspected causes of the events. The only way to reduce the risk to zero is however to stop the activities creating the risk. This do in most cases depend on the business' willingness to give up some of their fundamental working processes [37].
- **Reducing the consequences of an adverse event:** This is done by limiting the damage the event causes. This can prevent the damage from spreading, or to shorten the time in which the event is active by accelerating detection and recovery times [37].

Information security technologies focuses primarily on risk mitigation. Information security risk analysis processes are directed towards imagining and then confirming technical vulnerabilities in information systems, so that measures can be taken to mitigate the risks these vulnerabilities create[37].

8.3.4 Retention

If the adverse event are not very costly nor very likely to happen, or if the benefits from taking a risk is great, the business might choose to live with the treat of an adverse event. This can be done by setting aside funds to offset the cost of retained risks. If the business choose this approach it is said to be self-insured against the risk [37]. This is a fairly common risk management approach, in particular for smaller companies in the context of information security. A lot of companies even accept the risk without setting aside money to compensate for the risk experienced. They are said to accept retained risks [37].

[1] Definition from Barron's Finance and Investments dictionary

8.4 OUTSOURCING SECURITY MANAGEMENT

Blakely et. al. [37] posit that in the future, information risk should be treated by professionals with the characteristics of a physician. A physician has certain obligations and requirements:

- A specialized professional education.
- A revocable license to practice.
- An ethical obligation to treat patients appropriately and keep their private information in confidence.
- A professional obligation to control (through prescription) the use of potentially harmful treatments.
- A professional obligation to report, important public health information to the proper authorities.

This would be difficoult for smaller companies to have in-house. The need for a dedicated employee for information security would often not be severe. There are however possibilities to outsource these responsibilities.

8.4.1 Managed Security Services (MSS)

Small companies will in most cases to some extent benefit from hiring competency on security management [82]. The technologies and threats are increasing in complexity and causes smaller companies to seek help when attempting to secure their information. Managed Security Service Providers (MSSP) might be the solution for such companies. In managed security services, the security infrastructure of a client company is overseen or managed by a MSSP. [82].

The services the MSSP provides are for example [83, 84]:

- **Perimeter Management and Network boundary protection:** The service often includes installation and maintenance of firewalls, virtual private networks and intrusion detection systems. The vendor is responsible for installing and upgrading software and for configuring hardware, protecting the network boundaries. There are few service providers that are able to offer this service.
- **Managed Security Monitoring:** Involves monitoring the client's network and interpreting of the system events in order to identify malicious activity. Incident management and incidents response process are also in this category.
- **Vulnerability assessment and penetration testing:** Involves periodic port scans and hacking attempts in the clients network to identify vulnerabilities that could be exploited by attackers.
- **On-site consulting:** This might include management activities such as risk assessment, identifying requirements of security and development of security policies. It might also involve technical support on-sight.
- **Compliance monitoring:** Includes monitoring of events to identify violations that may have taken place in a company. It also monitors any unauthorized changes to application servers, web servers and firewalls [83].

- **Anti-virus and content filtering services:** Includes scanning for virus, worms and malicious code on the desktop, in e-mails and the network traffic. Spam-filtering might also be an additional services provided by the MSSP.

By outsourcing security to a MSSP, a company can improve the uptime of their system while avoiding investments in resources and technology [85]. There are certainly possibilities for cost savings, also for smaller companies. Since MSSP's offer same functionalities and services to many clients, there are possibilities to negotiate good prices for clients due to economics of scale. I have gathered some information on the prices of these services delivered by Norwegian companies. These data relates to small companies. The pricing of such services are typically a start up cost, including documentation of the network and computersystem, risk evaluation etc. at NOK 20 000 - 40 000 and then a monthly fee of NOK 4 000 - 20 000 depending on the measures needed.

According to the former CEO of Coradiant, Alistair Croll,

> "Outsourcing security offers economies of scale, but also economies of skill, since it would cost much to hire full-time security experts"[86].

MSSPs are often very competent people with the best technologies to work with and the best knowledge of new incoming threats. It is also important to know the downside of MSS. It may be difficult to build trust with the MSSP, since they need access to most of the compnany's information to do their job. It is also a possibility that hidden costs will occur during the time period the MSSPs are delivering services. Due to this it is important to consider the option of having in-house competency as well. To avoid unwanted situation it is highly important to maintain a good dialogue with the MSSP at hand. Not only to make sure they are doing what they should, but also to avoid blaming games if something goes wrong. The in-house resources typically know more about the local network and changes, while MSSPs often know more about the global development in information security. Read more about Managed Security Services in [86, 85, 84].

CHAPTER 9
COST AND VALUE

One of the earliest used estimators in the computer industry was Annual Loss Expectations (ALE), a quantitative method for performing risk analysis [87]. The method was criticized because of the ”lack of empirical data on frequency of occurrence of impacts and the related consequences” thus producing an interpretation of ”results as having more precision than they actually had” [88]. ALE is described in section 9.1.

In recent years Cost-Benefit Analysis (CBA), such as Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR) has been used in the budgeting of information security investments. These methods are described in section 9.2.

This chapter will also present a model companies might use to determine how they should invest in information security, section 9.3. This model is particularly good for smaller companies with less employees and less information to secure, since it might be easier to identify their weakest links and demand of security. It should however also be adequate to use for larger companies as well, if the administration and management of the companies are well taken care of. The model starts identifying the calculated risk and the companies willingness to pay. Then we have to rank the different possible security measures in some way to decide which of them to prioritize the highest.

9.1 INFORMATION RISK

Blakely et. al. [37] states that today's security technologies do not reduce information risk very effectively. They propose that we need to reconsider our approach to securing information, to be able to secure information in a better manner in the future. First and foremost we need to be able to measure the risks. Compromise of valuable information assets introduce cost whether acknowledged or not. It might be direct losses; reduced value of the information itself, or indirect losses, such as:

- Service interruption
- Damage of reputation
- Loss of competitive advantage
- Legal liability
- Loss of work hours due to repair and damage control

Risk calculation methods most frequently used in “Willingness to pay” calculations in the line of insurance and medicine will be presented.

9.1.1 Measuring Risk

The term risk in the context of businesses can be defined as follows [37]:

> "The possibility of an event (adverse event), which would reduce the value of the business were to occur."

Every risk has a cost. This cost can be quantified in a more or less acurate manner. The cost of a particular risk happening during a calculated time period, is the probability that an adverse event will occur during this period of time, multiplied by the consequence this gives. The consequence is the amount of money the reduction in business value; direct or indirect loss [89].

A common measure of the cost of risk is *Annualized Loss Expectancy (ALE)*. ALE is the expected cumulative cost of risk over a period of time, and can be determined according to the following formula:

$$ALE = AssetValue \times ExposureFactor \times Frequency \tag{9.1}$$

The asset value is the total value of an asset or the cost of a successful attack where all information is compromised. The exposure factor is the percentage of the asset's value that is exposed and the frequency is the annual rate of occurrence. The calculation presuppose that the business is able to estimate these data accurately, based on earlier experience and research.

Quantitative information security risk management standards, described in section 8.1, have been developed to help companies measuring their risks. It is however important for companies to focus on optimizing cost of risk, rather than to minimize the probability of occurrence of adverse events.

9.1.2 Risk Measuring Example

Consider a very small organization with 5-10 employees, with medium to high value of information. The method requires the company to be able to make good estimation of their own information and asset value and calculated risk of security breaches, this can be done by looking at experience from resent years or by looking at results from similar companies. It might also be useful to consider results of surveys from resent years. Based on data from [**?**] The following data will be used:

$AssetValue = 1000000$

$ExposureFactor = 0.5$

$Frequency = 0.03$

The ALE will then be :

$$ALE = 1000000 \times 0.9 \times 0.07 = 63000 \tag{9.2}$$

This information is based on a situation where all of the information and assets are compromised in addition to work hours and business loss due to the attack. Considering that 90% of their total value are compromised as a worst case scenario, and using the estimated probability of a strike against such companies from [**?**]. The data this estimation are based on are, reported number of unauthorized use

of ICT-recourses (both account access and root access) and improper use. There are no such data for malware frequency, but this is normally higher than the other two. There are therefore added an additonal amount for this as well. There are less incidents reported in the 2006 survey than in the two previous surveys. Because of this the ammount could be reduced, but since the recipients probably already have some measures installed it is keept as it is to compensate for this.

All in all, the calculated willingness to pay for the firm is approximately NOK 63 000.

9.2 INFORMATION SECURITY BUDGETING

The cost associated with information security activities relates to many items, including:

- Software
- Hardware
- Personel

Most of these expenses are best thought of as capital investments, although most companies tend to treat these cost as operating expenses within the current period. Whether they look at the expenditures one way or another, the question of information security budgeting is a crucial resource allocation issue. From an economical perspective, firms should invest up to the point where the last dollar of information security investments yields a dollar of savings [90]. Information security expenses should be viewed in cost-benefit terms.

The use of the net present value (NPV) model is common in budgeting and investment decision process in most industries. In the 2006 American Computer Crime Survey, this is actually the least used method in competition with Return on Investment (ROI) and Internal Rate of Return (IRR), see figure 9.1. Out of the 512 respondents in this survey, 82% reports that they are using some kind of investment analysis method, when taking budgeting decisions regarding information security [7].

9.2.1 Return on Investment (ROI)

Gordon et.al. describes in [91] why the simple return on investment (ROI) calculation are insufficient. This statement is based on that since ROI is based on historical rather than future valuations. The ROI is obtained by the simple formula [92]:

$$ROI = \frac{Y(t)}{V(t-1)} \tag{9.3}$$

for $V(t-1) \neq 0$

where:

$Y(t)$ = income of the period

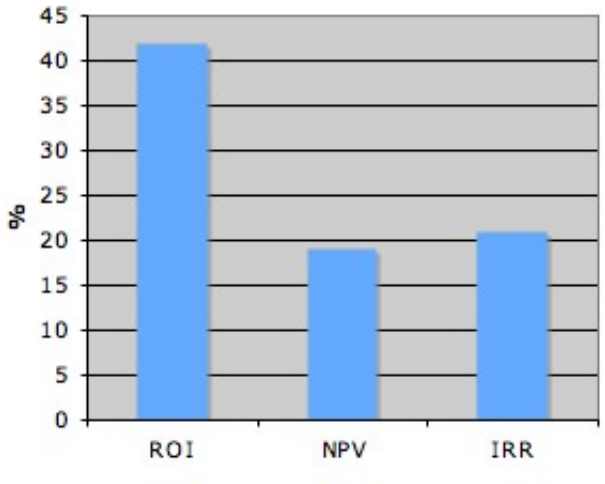

Figure 9.1: Percentage of organizations using ROI, NPV and IRR metrics [7].

$V(t-1)$ = present value of the asset at the end of previous period

The rapid evolvement in the information security industry, might cause the organization to base their decisions on wrong assumptions. There are however a trade-off between counting on past data and predicting the future.

9.2.2 Net Present Value (NPV) Model

For most managers it is better to get a dollar in the hand today than to get a promise of two dollars in one year. They encounter a risk that the dollars never will be paid, if they have to wait for a year. In the same way, most managers think it is better to pay an amount of money to secure they information today, than encountering a bigger risk of a huge cost if the information gets compromised in one year. It is not certain that this will happen, and it is not certain that it won't happen if they pay some money for security measures, they are however reducing the risk of substantial loss.

This is the basics behind calculations of the NPV. The NPV are calculated using the following formula [92]:

C_t = cash flow at the end of period t

i = time value of money of the firm

r = internal rate of return of the investment

NPV = net present value of the investment

n = life of the investment

$$NPV = \sum_{t=0}^{n} C_t(1+i)^{-t} \tag{9.4}$$

9.2.3 Internal Rate of Return (IRR)

The internal rate of return method utilizes present value concepts. The procedure is to find a rate of discount that will make the cash proceed expected from an investment equal to the present value of the cash outlays required by the investment. Using the same parameters as in the previous subsection the IRR is calculated using one of the following equations [92]:

$$\sum_{t=0}^{n} C_t(1+r)^{-t} = 0 \tag{9.5}$$

$$\sum_{t=1}^{n} C_t(1+r)^{-t} = -C_0 \tag{9.6}$$

9.3 My Approach to the Investing Problem

Because most CEO's actually have economical backgrounds and mostly not any technological education, they are probably more comfortable with terms such as cost-benefit, risk, and other economical conceptions. It might therefore be more comfortable for them to discuss information security in an economical perspective.

9.3.1 Willingness to Pay

Gordon and Loeb demonstrates in [20] that "under certain sets of assumptions concerning the relationship between vulnerability and the marginal productivity of the security investment, the optimal investment in information security may either be strictly increasing or first increase and then decrease as vulnerability increases." Because of this, under plausible assumptions, it might be right to only invest in a midrange of information vulnerabilities. Little or no information security is economically justified for both extremely high and extremely low levels of information vulnerability, see section. The ICT-management then need to take a choice of retention (subsection 8.3.4).

The use of ALE might give a good indication on the willingness to pay for information security. However, this does not take the different levels of vulnerability of the information might have into account. ALE is easy to use, and should be good enough for most smaller companies. Although, due to the weakness of AOL an alternative method for finding the optimal amount of investments in information security will be presented.

According to common microeconomic principles, the optimal investment, is where the difference between benefits and costs are maximized [93]. This optimal point is found by the following method, based on a one-period case, parts of this model is from [20], that also gives a more thorough analysis of optimization of investment :

Defenition of variables: α = The loss if an adverse event occurs, this loss representing the different levels of information values described in section 3.3.
p = The probability of an adverse event occurring
q = The vulnerability of the information, probability for a successful attack

It is assumed that α have a limit, and thereby ignoring the adverse events resulting in catastrophic immeasurable loss.

Defenition of the potential loss associated with a set of information:

$L = \alpha p$
I = the money invested in information security

And $F(I, q)$ is the probability that an information set with the vulnerability of q will be breached, when the organization has invested an amount of I in information security. The formula for reduced expected loss will now look like this:

$$REL(I) = [q - F(I, q)]L \tag{9.7}$$

The investment in information security is the company's only decision variable.

The total net benefit from the investment will be equal to REL minus the investment I.

$$NREL(I) = [q - F(I, q)]L - I \tag{9.8}$$

The optimal investment would be denoted $I^*(q)$. The equation $F(I, q)$ is assumed to be strictly concave since the more you invest the more secure the information gets, but by an decreasing rate. Due to this, the interior maximum $I^* > 0$ is characterized by the first order condition [92]:

$$-F_I(I^*, q)L = 1 \tag{9.9}$$

where the left side represents the marginal benefit from the security investments and the right hand side represents the marginal cost of investment. As you can see

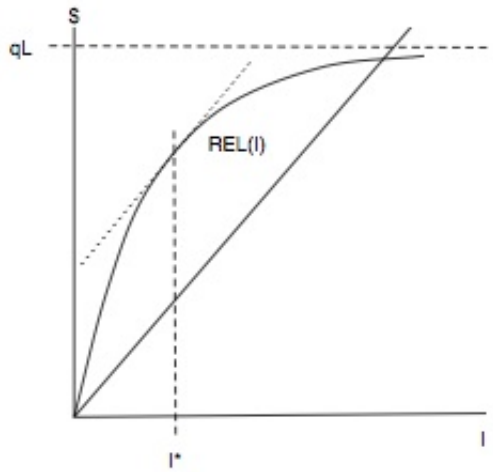

Figure 9.2: Level of investment in information security [20].

in figure 9.2 it will only be beneficial to invest small fractions of the estimated loss when attacked.

9.3.2 What Should The Firm Invest In?

In this section an approach where you first decide the optimal amount of money to invest in information security, based on the assets of you information are consid-

ered. This can be done using AOL or the optimization model presented benefit/cost - model presented earlier. When this data is calculated, there is a need to decide what information security measures to choose. To decide the model in this section will consider different protection approaches to different sets of information as "projects" in the investment analyzes theory. The projects to choose from need to be prioritized according to some known procedure. This is done using either of the methods presented in section 9.2. In this concept case ROI is used, even though this is said to be inefficient. Combining the result from last period with the expectations of the next according to trends, should result in an efficient enough model.

The first step is to find all alternatives, and eliminate those that certainly will not be chosen after the prioritizing. It is important to take into account what Gordon and Loeb discovered in [20]; the most and least vulnerable information, will in almost all cases not be beneficial to spend money to protect.

By setting up a matrix of the known threats and the known security measures and assigning rates according to how well the measures are at identifying problems, you quickly get an overview of the values needed for the calculations. These rates are called *Bypass rate (BR)*. "Bypass rate is the rate at which an attack results in observable damage to the organization. Each security solution has a bypass rate for every incident type" [94]. A 100 percent bypass rate means that the security solution do not stop any attempts of the incident type and is denoted by the number 1.0. There are no official numbers based on statistics, but if this method would become used by many, it would be beneficial to have government standards as guidance. Companies typically categorize incidents regarding network security in four types [94]:

- Account compromises: unauthorized account access
- Improper use: information leaks and other potential embarrassments to the organization
- Malicious code infections: such as worms and viruses
- Root compromises: unauthorized root access to user accounts

These are represented in the bypass rate matrix in table 9.1. It is also necessary

	Account compromises	Improper use	Malicious code infections	Root compromises
Firewalls	0.80	1.00	0.80	0.80
Vulnerability eradication program	0.40	1.00	0.40	0.40
Intrusion prevention system	0.15	0.15	0.15	0.15
Training program	0.70	0.70	0.70	0.80
Introduction of policies	0.50	0.40	0.80	0.50
Net bypass rate	0.0192	0.048	0.03072	0.0216
Observed damage (NOK)	5000	25000	100000	60000
Incident risk (IR) (NOK)	260400	520800	3255200	2777800

Table 9.1: Categorization matrix for small companies, partially from [94] and from the complete numbers of [28]

to gather information on the cost of the alternative security implementations. The cost is represented by c_s for the remaining of this section. These numbers will be estimated and the calculations continued in subsection 9.3.3.

When all of these data is gathered, the next step is finding the priority of the security measures considered. By adding all of the incidents risks in table 9.1 the total amount of risk encountered with no security solutions implemented are presented. This is denoted RN for the rest of the section. Now it is time to reduce the risk as much as possible with the available money. The first step towards this is calculating the residual risk for each security solution with the following formula where BR_{11}, BR_{21}, BR_{31} and so on are the bypass rates for the considered solution for breach type 1, 2 and 3:

$$RR(s=1) = (BR_{11} \times IR_1) + (BR_{21} \times IR_2) + (BR_{31} \times IR_3) + (BR_{41} \times IR_4) \quad (9.10)$$

To determine the residual risk when more than one solution is implemented use:

$$RR(s=1,2) = (BR_{11} \times BR_{12} \times IR_1) + (BR_{21} \times BR_{22} \times IR_2) + (BR_{31} \times BR_{32} \times IR_3) \ldots \quad (9.11)$$

Net benefit for the security implemented are:

$$NB(s) = NR \times RR(s) \times c_s \quad (9.12)$$

Calculation of the Ratio Return on Investment (RROI):

$$RROI(s) = \frac{NB(s)}{c_s} \times 0.01 \quad (9.13)$$

If the company has a roof of investment, calculated by ALE or similar, they need to add up the cost of the best security measures based on the RROI until they have filled the budget. They might however also have no roof but a least acceptable limit of risk, then they need to add the measures with the best RROI's until this goal is reached. The methods described in subsection 9.3.3 will be used as a proof of concept with estimated data.

9.3.3 Proof of Concept

It is assumed that the company has a limit of willingness to pay, and use the amount (NOK 63000) calculated in subsection 9.1.2. After some research estimated prices on the different services are provided, these are based on numbers from a Norwegian security service provider and the measures and hardware they would recommend with the scenario described. The prices are presented in NOK in table 9.2. Firstly it is neccesary to find the baseline scenario of the problem, which is the sum of all the incident risks:

$$260400 + 520800 + 3255200 + 2777800 = 6814200 \quad (9.14)$$

Finding the residual risks for all of the measures in table 9.2:

$$RR(Firewall) = (0.8 \times 260400) + (1.0 \times 520800) + (0.8 \times 3255200) + (0.8 \times 2777800) = 5555520 \quad (9.15)$$

$$RR(VEP) = (0.4 \times 260400) + (1.0 \times 520800) + (0.4 \times 3255200) + (0.4 \times 2777800) = 3038160 \quad (9.16)$$

$$RR(IPS) = (0.15 \times 260400) + (0.15 \times 520800) + (0.15 \times 3255200) + (0.15 \times 2777800) = 1022130 \quad (9.17)$$

Measure	Method	Hardware cost	Other cost
Firewall	FortiGate–50B	6000 + tax	4000 (config)
Vulnerability eradication program	With web application check	0	50000 (consultant cost)
Intrusion prevention system	Part of FortiGate–50B	0 if firewall chosen	0 if firewall chosen
Training program	Training	0	10000 (fee) + 10000 (loss of work hours)
Introduction of policies	In-house	0	7000 ($salary \times hours$)

Table 9.2: Prices of security measures for a company with 5-10 employees and medium-high information vulnerability.

$$RR(Training) = (0.7\times260400)+(0.7\times520800)+(0.7\times3255200)+(0.8\times2777800) = 5047720 \tag{9.18}$$

$$RR(Policy) = (0.5\times260400)+(0.4\times520800)+(0.8\times3255200)+(0.5\times2777800) = 4331580 \tag{9.19}$$

Then the net benefit for all of the above measures needs to be calculated. The price of the firewall and intrution prevention system are set to be the same, since both are provided at a mutual cost. This price is uncluding consultion cost for configuration and updates: $NB(Firewall) = 6814200 - 5555520 - 12000 = 1246680$

$NB(IPS) = 6814200 - 1022130 - 12000 = 5780070$

$NB(VEP) = 6814200 - 3038160 - 50000 = 3726040$

$NB(Training) = 6814200 - 5047720 - 20000 = 1746480$

$NB(Policy) = 6814200 - 4331580 - 7000 = 2475620$

The last thing needed to done before prioritizing the measures are possible is to calculate the PROI:

$$PROI(Firewall) = \frac{NB(Firewall)}{Price} = \frac{1246680}{12000} = 103.89 = 10.4percent \tag{9.20}$$

$$PROI(IPS) = \frac{NB(IPS)}{Price} = \frac{5780070}{12000} = 481.67 = 48.2percent \tag{9.21}$$

$$PROI(VEP) = \frac{NB(VEP)}{Price} = \frac{3726040}{50000} = 74.52 = 7.5percent \tag{9.22}$$

$$PROI(Training) = \frac{NB(Training)}{Price} = \frac{435060}{20000} = 87.32 = 8.7percent \tag{9.23}$$

$$PROI(Policy) = \frac{NB(Policy)}{Price} = \frac{2475620}{7000} = 353.66 = 35.4 \tag{9.24}$$

Look at these results the organization at hand seems to benefit from investing in IPS firstly. Then they will get the firewall for free. This introduces a cost of NOK 12 000. So the company are able to invest in more security. Next up is the introduction of policies at a cost of NOK 7000. All together the cost of security are now 19 000 so the company can afford to take their employees to a training event as well, in total cost this will be 39 000, and there is no room for investments in VEP. All in all, this gives a risk (NOK) on:

RR(tot) = (0.8$\times 0.15 \times 0.7 \times 0.5 \times 260400$)
$+ (1.0 \times 0.15 \times 0.7 \times 0.4 \times 520800)$
$+ (0.8 \times 0.15 \times 0.7 \times 0.8 \times 3255200)$
$+ (0.8 \times 0.15 \times 0.8 \times 0.5 \times 2777800) = 384900$

In addition to IPS the firewall also includes virus detection, e-mail filtering and VPN, the residual risk is probably even lower than indicated in the calculated numbers.

CHAPTER 10
DISCUSSION

There is no such thing as two identical organizations. Every single one has it's own assets, weaknesses, employees and fundamental strategies. This makes each company's requirement for ICT-systems and information security identical as well. One solution might be good for one company but not for others. The differences in organizational structure and mentality is important variables in the process of building a good and secure infrastructure for the organizations.

Size is an important parameter. This thesis are mainly focusing on smaller companies and their investments in information security, defined to include companies with 1-50 employees. This definition is based on European standards, and do probably include to many companies compared to Norwegian scales. Analyzing results from surveys performed all over the world; smaller companies are less likely to experience adverse information security events. However, when these occur they are more likely to be successful. This is probably a result of the companies reduced willingness to pay for security and the fact that they take new technology into use considerably later than bigger companies.

The reason for this elevated success rates in smaller companies, is also a result of the lack of in-house ICT-employees. The smaller companies do often not have any dedicated workers taking care of ICT and information security. Mostly one of the co-workers only has an extended responsibility for these matters, in combination with it's main position in the company. In these cases the ICT responsibility often get low priority and very little time is spent improving the companies security by for instance making policies, installing new security patches etc.

There are alternatives for those companies without in-house ICT expertise. Managed Security Services is a term including all forms of outsourcing information security. For smaller companies this may be to costly, but economics of scale makes it possible for smaller companies to get good deals on these services. There are however a trade of between hireling help and using own personnel. The employee of the company often know the local infrastructure, content and mentality towards ICT, while managed security service providers are more up to date on the global changes in information security. It is therefore very important to maintain good communication between the MSSP and the client to optimize use of both parties knowledge.

The Australian Computer Crime Surveys [3, 4] presents four readiness to protect factors, these are: Technology, policies, training and standards. These factors are used as a template for this thesis. If companies focus on these four aspects of information security, and succeed in combining it in an optimal manner they are said to have security in depth. There is no use in investing great amounts of money on technology if these are not used in a justifiable manner.

There are many technological security solutions to choose from. Passwords (authentication), virus-controls, firewalls and back-up are the four most commonly used. All of these measures provide good protection if they are properly used, and can prevent many attempted attacks. Firewalls and Virus-controls do however often base their operations on previously known abusive patterns. They will therefore have some shortcomings and difficulty discovering new threats.

Mobile threats are expected to increase the following years. More and more information are available through mobile devices, making it an interesting target for computer criminals. The use of common languages such as Java on mobile applications, have increased the risks of intrusion. There are expectations of similar development in mobile threat as the development on threats in PC in the 90's. Despite the fact, it do not seem that the lessons learned back then are utilized to stay a head of the attackers. There are few security measures available for mobile devices, and very few users of the existing ones. Mobile phones get increasingly advanced due to introduction of new features. This has led to a new term, smart phones. Most of the newly introduced features in smart phones are access points for potential mobile malware. Not even simple measures such as careful use of Bluetooth are taken to prevent adverse events. This is assumed to be due to lack off knowledge. Certain devices are actually sold with this feature turned on, and many users not aware of the functionalities they smart phone have, do not turn it off.

Proper use of technologies is a prerequisite for their provided security. Lack of knowledge is only one reason for unjustifiable use of technical resources. This can be limited by training of employees. Laziness and carelessness are two other reasons not as easy to address. There are however training methods presented as simulator games available. CyberCIEGE is an example of this. CyberCIEGE present the training attendants for unexpected and unwanted situations. These situations can be a result of careless use, and the player need to prevent the event from doing to much damage. Even though a video game, expecting more of users than simple mouse clicks often get to complicated for inexperienced users, this method seem to be helpful in providing better awareness among employees. The new generations are presented to video-games at early stages in life, and computers become common knowledge in today's digital age. There are however differences in opinion on to what extent it is possible to change users behaviors in later stages of life. Children are more adaptive to changes and are faster learners. There are suggestions that information security attitude need to be addressed as early as in middle school, to be able to change the common behavioral problems in information security context.

Policies are also a way to help improve employees awareness towards information security. Formalizing the rules when using ICT-recourses, can be the first step towards a more secure business. The supposition is of course that employees actually reads them, and take notice of the presented information. Policies is in particularly useful when new employees are joining companies. It is difficult to manage to give an oral presentation without forgetting any of the necessary information about the use of ICT. Policies is a way of bringing structure in the ICT strategies and common attitudes in companies.

Use of standards is another way of bringing structure into ICT-operations in a company. Compared to policies, the standards are mainly meant for ICT-personnel and management and not for all the employees in the company. There are many standards provided, both local standards provided for separate countries and global standards. Results from the Australian surveys give indications that increased use

of standards, reduce incident rates. The main objectives of most standards are to give guidance on how companies can be able to find their own information security risks, how to limit or prevent damage caused by adverse events, and how to calculate the total loss due to information security breaches.

Even though these standards are available to everyone at no or low cost, one of the first discoveries of this thesis is the companies inability to estimate data, related to risks and losses. These data are essential in the information security investment analysis, and wrong, inconclusive or nonexistent estimates may lead to useless results. As long as companies to little extent calculate and report their losses when adverse event happens, it will be difficult to give advice on which security measures are most useful and which are not useful at all. The surveys presented in this thesis might be at help estimating numbers for budgeting calculations. It is however a relatively small amount of respondents, and the survey is not mandatory. The answers given are not in any matter verified. This might lead to inconclusive information. A government initiative may be able to help gather more reliable information. By making it mandatory for companies to answer questionnaires concerning information security on a regular basis, they can be able to present data appropriate for each companies investment calculations. This do however imply that the government need to invest in a more secure ICT future. Since information security in many cases are just as much or even more a matter of public than private security, this is a cost the governments should be willing to take.

The management of small businesses is often in charge of the security management as well as the day to day operation of the organization. Chapter 8 presents some of the most important decisions a manager need to take regarding information security. First of all it is necessary to choose a good model for access control. Who should have access to what information when? In smaller companies of 1-3 people, this may in some cases not be an issue. If the business grows the managers should however make decisions on what the companies access policies should be like. The management also need to take a decision on how the firm apply to risk. Smaller companies are often risk adverse, deciding to accept the risk, without any precautions or actions in reducing this. This seems in particularly to be the most beneficial approach if the company assets are of very low or very high value. If the value is high, the cost of securing it will extend calculated risk, and lead to a reasonable economical decision to not secure it. Medium valued assets, are however mostly handled by mitigation, that is, trying to limit the risk of an adverse event taking place, or reducing the cost if it does.

The security investment model presented in this report relies in the companies ability to present trustworthy data. It is also based on the fact that smaller companies often are very vulnerable to big expenses. They usually do not have a lot of money to spend, and their information security budget are therefore not that big. Small differences in budget and punctuation can mean a lot, but so may the loss of time, loss of information, or loss of customers. Firstly the model finds maximum amount the company is willing to spend in securing their information. This is done using ALE or cost/benefit equilibrium method. Secondly there is a need for prioritizing different security solutions relevant for the company. By defining the different security measures as the “projects” in traditional investment analysis, and applying ROI, NPV or IRR on these projects the best suited and profiting measures are easily found. The prices of the security solutions often involves a one-time cost, and additional annual costs such as renewal of service agreement, annual software updates or regular maintenance fees. This count for a multiperiod model, which is easily implemented with any of the investment methods.

A one period ALE/ROI method are described to more extent in section 9.3. This method relies on bypass rates, that is the penetration rate of attacks through defined security measures. The bypass rates for existing and proposed security solutions may be difficult to estimate because of minimal or nonexistent information.

> "Currently, the most reliable sources of this information are intrusion detection experts who have worked closely with the particular solution and have detailed knowledge of the current security system.[94]"

In particularly this is true when evaluating new solutions. These often do not have actual performance data. The use of honeypots as network traps have however made it possible to measure the potential frequency on certain networks in an accurate way. This method combined with more extended use of logging and reporting incidents to an authority, might able bypass rates to be more accurate measures in the investment decision making process.

CHAPTER 11
CONCLUSION

The main goal of this project has been to address the need for an investment analysis model that supports the individual principles of small businesses and organizations. I have studied a set of investment decision tools, none of them do however relate to small companies in particular. Despite the limited time and capacity on this thesis and the lack of earlier published proposals, I have learned to understand the problems at hand and managed to make a suggestion on a method that should address some of the problems in security budgeting decision making processes.

The reason why there is a need for such models are the fact that smaller companies simply do not spend much money on information security. Even though less small companies experience adverse events, the attacks on these businesses are more likely to succeed. The fastest growth in use of ICT services are in the smaller organizations, despite this they seem to fall behind in the security area. This is in some cases a calculated decision based on the possible losses, but in most cases there is no such strategy at hand. They simply do not know about the dangers they encounter.

The first discovery was the companies inability to calculate their own risks and total losses when incriminated. To be able to make accurate calculations of the benefits of security measures, these numbers are critical. Most smaller companies do not even know if their systems have experienced unauthorized use during the last year, and do not log unwanted incidents. The incidents they are aware of are most of the time not reported to the authorities, which makes it hard to gather information on the overall situation, and provide statistics the companies will be able to use in their own risk analysis. To be able to address this it would be necessary with a government initiative to help smaller companies that do not have the recourses, ability or willingness to take action on their own. This instance should provide guidelines for calculations, and make it mandatory to answer surveys and report incidents each year. If this were followed through they would also be able to provide estimates that companies might use in their budgeting decisions.

A lot of incidents happen because of wrong or unjustifiable use of ICT recourses. This is due to lack of knowledge, because of laziness, or bad attitude towards information security. This shows that it is impossible to be secure from intruders and adverse events by only spending money on technologies. Security in depth is an important term, implying that the companies need to take measures in all levels of their organization to be able to reduce risk of intrusion. Lack of knowledge is easier to address than the carelessness. Use of new training systems, where the attendants experience the threats in simulated situation might however be a wake up call for those employees unwilling to follow stated policies in companies. It is reason to believe they will be more careful when knowing the damage their carelessness might lead to.

The security investment model presented in this report relies in the companies ability to present trustworthy data. Smaller companies do often have very limited amount of money to spend in general, and therefore also on information security. Due to this an investment analysis model which take the maximum amount of spendable money into account are chosen. The model have certain limitations due to the lack of relevant information about historical events, but provide an insight on how smaller companies should evaluate their need for information security. The calculations only consider a few security services but the model is easily expanded to involve additional ones. However, there where discovered a benefit in investing in firewall implementation, intrusion detection programs, training and introduction of policies. These results might however be different if new measures are introduced, such as back-up, virus-controls, spam-filters etc. The model allows for introduction of these new measures by recalculation of properties and prioritizing these new ones.

CHAPTER 12
FUTURE WORK

This chapter presents some of the shortcomings of this thesis, and suggests future work to eliminate these.

12.0.4 Scenario Methodology

When defining the scenarios both for the outlook of the future and for the proof-of-the-concept case there are used different methods for scenario development, fitting the purpose of the scenarios (section 2). All of these methods have one thing in common; it is strongly recommended to work in teams, consisting of people with different expertise and experience. Even though the matter is discussed with different people, the scenarios are mostly developed by alone. This is a potential weakness in the thesis. By developing these scenarios single handed, one might get subjective opinions, which might lead to narrow outcomes.

This thesis would therefore probably be enrichened if the scenarios where a result of team work. It would be interresting to compare such scenarios to mine.

12.1 THE UNCERTAINTY OF THE SURVEYS

Today, some data on risk prevalence and severity is collected by the US FBI, CERT, Norwegian National Authority for the Investigation and Prosecution of Economic and Environmental Crime and other organizations. However, reporting to these organizations is voluntary, and only a small sample of businesses even receive the questionnaires which these bodies use to collect their summary information. Furthermore, no standard taxonomies of vulnerabilities, incidents, losses, or countermeasures are used in the collection or reporting of this information.

12.1.1 Public Security Service

To be able to gather useful information that can be helpful in the investments analysis in organizations, it is probably needed to collect information more regularly and structured in the future. Information risk should be analyzed and studied by an independent body, in the same way as public health service. This authority should take a in-depth study of the characteristic, and use this data to help businesses become more secure. Most smaller companies simply do not have the money, find the risk of being attacked to low, or do not have the competency to protect themselves from malicious activity. If we do not “feed” the intruders, they will no longer benefit from their activities.

12.2 THE MODEL

The model described in chapter 9 do not take into account how potential attackers of an information system change strategies in reaction to an additional security investments. That is, the analysis does not consider the game theoretic aspects of information security. The model contains strictly static properties, but would most certainly be more accurate if it where able to include dynamic issues, such as effects of changes due to security breaches.

Introduction of such parameters would conduct an even more accurate budgetting decission calculation, useful in fighting computer crime.

Bibliography

[1] "2 delen av alle føretak (5-9 sysselsette) med tilgang til internett, etter næringsområde. 2001-2006. prosent." visited: 15.05.07 created: 15.09.06.

[2] "Ikt-norge, undersøkelse om it-sikkerhet," tech. rep., Visendi AS, 2007. Prosjektleder: Jens Fossum, Metode: Hege Monho, Analyse Knut Egil Veien.

[3] "2006 australian computer crime and security survey," Tech. Rep. 5, Australian Computer Emergency Response Team (AusCERT), 2006.

[4] "2004 australian computer crime and security survey," Tech. Rep. 4, Australian Computer Emergency Response Team (AusCERT), 2004.

[5] T. Eriksson and T. Ritchey, "Scenario development using computerised morphological analysis," *Cornwallis and Winchester International OR Conferences*, 2002.

[6] "Mørketallsundersøkelsen 2003 -om datasikkerhet og it-sikkerhet," Tech. Rep. 4, Økokrim, Næringslivets sikkerhetsråd og Senter for informasjonssikkerhet, 2003. MY CONTACT: Kim Ellertsen, adm.dir in NSR.

[7] "Csi/fbi computer crime and security survey 2006," Tech. Rep. 11, Computer Security Institute (CSI) and Federeal Bureau of Investigation (FBI), 2006.

[8] D. Johnson and H. Koch, "Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive?," *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*, vol. 6, 2006.

[9] "Csi/fbi computer crime and security survey 2005," Tech. Rep. 10, Computer Security Institute (CSI) and Federeal Bureau of Investigation (FBI), 2005.

[10] W. Stallings, *Network Security Essentials*. Prentice Hall, second ed., 2003.

[11] Microsoft, "Using access control lists," tech. rep., Feb 2006. `http://www.microsoft.com/technet/prodtechnol/sppt/sharepoint/reskit/part2/co8spprk.mspx`.

[12] M. Burmester and Y. Desmedt, "Is hierarchical public-key certification the next target for hackers?," *Communications of the ACM*, vol. 47, no. 8, pp. 68–74, 2004.

[13] M. Hypponen, "Malware goes mobile," *Scientific American*, 2006.

[14] T. Karygiannis and L. Owens, "Wireless Network Security," *NIST Special Publication*, pp. 800–48, 2002.

[15] C. Irvine, M. Thompson, and N. P. S. M. CA, *Teaching Objectives of a Simulation Game for Computer Security*. Defense Technical Information Center, 2003.

[16] "Recognize phishing scams and fraudulent e-mails." published: 18.10.06 visited: 15.05.07.

[17] B. Shepard, "Information Security - Who Cares?," 2002.

[18] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224–274, 2001.

[19] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[20] L. Gordon and M. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[21] W. R. Adrison, "Reasearch methododology in software engineering, summary of the dagstuhl workshop on future directions in software engineering," *Software Eng. Notes*, 1993.

[22] R. Glass, "A structure-based critique of contemporary computing research," *J. Systems and Software*, 1997.

[23] E. H. Forman and M. A. Selly, *Decision by Objectives, how to Convince Others that You are Right*. World Scentific Publishing Co. Pte. Ltd., 2001.

[24] Shell, "Scenarios; An Explorer's Guide," *2001 Global Sceanrio Project*, 2001.

[25] F. Zwicky, "Discovery, invention, research - through the morphological approach," *Brussels*, 1969.

[26] T. Ritchey, "General morphological analysis, a general method for non-quantified modeling," *Brussels*, 1998.

[27] W. Stallings, *Computer organization and architecture*. Prentice Hall Upper Saddle River, NJ, 2000.

[28] "Mørketallsundersøkelsen 2006," Tech. Rep. 5, Næringslivets sikkerhetsråd, 2006. MY CONTACT: Kim Ellertsen, adm.dir in NSR.

[29] "Bedrifter og føretak." visited: 15.05.07.

[30] "Lov 1999-07-02 nr 64: Lov om helsepersonell m.v. (helsepersonelloven)," 1999. LATEST RENDERED: 2007-01-01.

[31] "Lov 2000-04-14 nr 31: Lov om behandling av personopplysninger. (personopplysningsloven)," 2001. LATEST RENDERED: 2001-01-01.

[32] "Lov 1995-08-04 nr 53: Lov om politiet m.v. (politiloven)," 1995. LATEST RENDERED: 2006-01-01.

[33] "Lov 1971-06-11 nr 52: Lov om strafferegistrering m.v. (strafferegisterloven)," 1971. LATEST RENDERED: 2003-07-01.

[34] "Lov 1981-05-22 nr 25: Lov om rettegangsmåten i straffesaker m.v. (straffeprosessloven)," 1981. LATEST RENDERED: 2006-07-01.

[35] "Lov 1998-03-20 nr 10: Lov om forebyggende sikkerhetstjeneste (sikkerhetesloven)," 1998. LATEST RENDERED: 2006-01-01.

[36] "Lov 1967-02-10 lov om behandlingsmåten i forvaltningssaker m.v. (forvaltningsloven)," 1970. LATEST RENDERED: 2005-01-01.

[37] B. Blakley, E. McDermott, and D. Geer, "Information security is information risk management," in *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, (New York, NY, USA), pp. 97–104, ACM Press, 2001.

[38] "10 delen av alle føretak som brukte ulike tryggingstiltak 2003–2006 prosent." visited: 15.05.07 created: 15.09.06.

[39] R. Smith, *Internet cryptography*. Addison-Wesley Reading, Mass, 1997.

[40] C. Nachenberg, "Computer virus-antivirus coevolution," *Communications of the ACM*, vol. 40, no. 1, pp. 46–51, 1997.

[41] D. Chess, "The future of viruses on the Internet," *Virus Bulletin International Conference, October*, pp. 1–3, 1997.

[42] A. Tanenbaum, W. Day, and S. Waller, *Computer Networks*. Prentice Hall, fourth ed., 2002.

[43] "Microsoft office sharepoint server 2007." visited: 18.05.07.

[44] N. W. Group, "Lightweight directory access protocol," tech. rep., dec 1997. `http://www.ietf.org/rfc/rfc2251.txt`.

[45] D. F. Ferraiolo, D. Kuhn, and R. Chandramouli, *Role-Based Access Control*. Artech House, first ed., 2003.

[46] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," *Advances in Cryptology–CRYPTO*, vol. 2729, 2003.

[47] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *Information Theory, IEEE Transactions on*, vol. 31, no. 4, pp. 469–472, 1985.

[48] "Digital signature guidelines tutorial." visited: 18.05.07.

[49] F. I. P. S. P. 186, "Computer virus-antivirus coevolution," *National Technical Information Service*, 1994.

[50] C. Adams and S. Lloyd, *Understanding Pki: Concepts, Standards, and Deployment Considerations*. Addison-Wesley Professional, 2002.

[51] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications*, 1978.

[52] F. Sebastiani, "Machine learning in automated text categorization," *ACM Computing Surveys (CSUR)*, vol. 34, no. 1, pp. 1–47, 2002.

[53] J. Kong, P. Boyking, B. Rczaci, N. Sarkar, and V. Roy-CHOWDHURY, "Scalable and reliable collaborative spam filters: harnessing the global social email networks," *Conference on Email and Anti-Spam*, 2005.

[54] H. Drucker, D. Wu, and V. Vapnik, "Support Vector Machines for Spam Categorization," *IEEE TRANSACTIONS ON NEURAL NETWORKS*, vol. 10, no. 5, 1999.

[55] M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz, "A Bayesian approach to filtering junk e-mail," *Learning for Text Categorization: Papers from the 1998 Workshop*, vol. 62, 1998.

[56] M. Wu, Y. Huang, S. Lu, Y. Chen, and S. Kuo, "A Multi-Faceted Approach towards Spam-Resistible Mail," *Dependable Computing, 2005. Proceedings. 11th Pacific Rim International Symposium on*, pp. 208–218, 2005.

[57] J. R. Segal and J. Crawford, "Spamguru: An enterprise anti-spam filtering system," in *In procedings of First Conference on Email and Anti-Spam (CEAS)*, 2004.

[58] J. Kong, P. Boykin, B. Rezaei, N. Sarshar, and V. Roychowdhury, "Let Your CyberAlter Ego Share Information and Manage Spam," *Arxiv preprint physics/0504026*, 2005.

[59] P. Ahonen and R. Savola, "Security threats to mobile service development in the age of digital convergen," *IEEE Eurocon 2005*, 2005.

[60] S. Janssens, "Preliminary study: BLUETOOTH SECURITY," 2005.

[61] S. Weatherspoon, "Overview of IEEE 802.11 b Security," *Intel Technology Journal Q*, vol. 2, 2000.

[62] "Logical link control and adaptation protocol, tutorial."

[63] M. Hentea, "A Perspective on Achieving Information Security Awareness," *Information Science and Information Technology Education. Flagstaff, Arizona, USA*, pp. 169–178, 2005.

[64] S. M. Furnell, A. G. Warren, and P. S. Dowland, "Improving security awareness through computer-based training," pp. 287–301, 2003.

[65] J. Pallant, *SPSS Survival Manual: A step by step guide to data analysis using SPSS*. Allen & Unwin, 2004.

[66] R. Summers, *Secure computing: threats and safeguards*. McGraw-Hill, Inc. Hightstown, NJ, USA, 1997.

[67] M. Bishop and M. Bishop, *Computer Security: Art and Science*. Addison-Wesley Professional, 2003.

[68] S. Pfleeger and C. Pfleeger, *Security in Computing*. Prentice Hall PTR, 2003.

[69] B. Cone, C. Irvine, M. F. Thompson, and T. Nguyen, "A video game for cyber security training and awareness," *Computers and Security*, vol. 26, pp. 63–72, 2007.

[70] C. Irvine, M. Thompson, K. Allen, and N. P. S. M. CA, *CyberCIEGE: An Information Assurance Teaching Tool for Training and Awareness*. Defense Technical Information Center, 2005.

[71] "Microsoft udate helps keep you computer current." published: 18.10.06 last updated: 10.04.07 visited: 15.05.07.

[72] "Ico/iec standards and patents." last updated: 18.04.07 visited: 24.05.07.

[73] A. Aizuddin, "THE COMMON CRITERIA ISO/IEC 15408–THE INSIGHT, SOME THOUGHTS, QUESTIONS AND ISSUES."

[74] I. Norma, "IEC 15408 (Common Criteria V2. 0)," 1999.

[75] D. Herrmann, *Using the Common Criteria for It Security Evaluation*. Auerbach Pub, 2003.

[76] M. V. Tripunitara and N. Li, "Comparing the expressive power of access control models," in *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, (New York, NY, USA), pp. 62–71, ACM Press, 2004.

[77] F. B. Schneider, "Enforceable security policies," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 1, pp. 30–50, 2000.

[78] T. A. Limoncelli and C. Hogan, *The Practice of System and Network Administration*. Addison Wesley, first ed., 2001.

[79] J. E. Tidswell and J. M. Potter, "A graphical definition of authorization schema in the dtac model," in *SACMAT '01: Proceedings of the sixth ACM symposium on Access control models and technologies*, (New York, NY, USA), pp. 109–120, ACM Press, 2001.

[80] W. Wang, "Team-and-role-based organizational context and access control for cooperative hypermedia environments," in *HYPERTEXT '99: Proceedings of the tenth ACM Conference on Hypertext and hypermedia : returning to our diverse roots*, (New York, NY, USA), pp. 37–46, ACM Press, 1999.

[81] J. D. Moffett and E. Lupu, "The uses of role hierarchies in access control," in *ACM Workshop on Role-Based Access Control*, pp. 153–160, 1999.

[82] A. Andress, *Surviving Security: How to Integrate People, Process, and Technology*. Auerbach Publications, 2003.

[83] S. Hunt, "Market overview: Managed security services," *Giga Information Group*, 2001.

[84] J. Allen, D. Gabbard, and C. May, *Outsourcing Managed Security Services*. Carnegie Mellon University, Software Engineering Institute, 2003.

[85] D. Deshpande, "Managed security services: an emerging solution to security," *Proceedings of the 2nd annual conference on Information security curriculum development*, pp. 107–111, 2005.

[86] E. DeJesus, "Managing Managed Security," *Information Security Magazine*, 2001.

[87] R. Mercuri, "Security watch: Analyzing security costs," *Communications of the ACM*, vol. 46, no. 6, pp. 15–18, 2003.

[88] "Guideline for the analysis of local area network security," 1994.

[89] S. Harrington and G. Niehaus, *Risk management and insurance*. Irwin/McGraw-Hill, 1999.

[90] L. Gordon and M. Loeb, "Budgeting process for information security expenditures," *Communications of the ACM*, vol. 49, no. 1, pp. 121–125, 2006.

[91] L. Gordon and M. Loeb, "Return on information security investments: Myths vs. realities," *Strategic Finance*, vol. 84, no. 5, pp. 26–31, 2002.

[92] H. Bierman and S. Smidt, *The Capital Budgeting Decision, Economic Analysis of Investment Projects*. Prentice Hall, 8 ed., 1993.

[93] A. Schotter, *Microeconomics: a modern approach*. Addison Wesley Longman, 2001.

[94] A. Arora, D. Hall, C. Piato, D. Ramsey, and R. Telang, "Measuring the risk-based value of IT security solutions," *IT Professional*, vol. 6, no. 6, pp. 35–42, 2004.