IT-Security Investment Models
Abstract

Threats to IT security are causing a lot of problems; companies without proper defenses and knowledge are falling behind and are losing money due to recovery costs. This research is aimed towards finding out how companies these days are investing, what investment models they are using to perfect their infrastructure for stronger IT security. This is done for the purpose of finding the most ideal model(s) for different types of companies to use.

Interviews were done with 12 companies to find out how they handle their investments, the most popular existing models and models still in development were analyzed to see what actually is included for the calculations for these models. The companies interviewed for the most cases did not know about the models that exist for investments in IT security, some let outside security consults handle their investment planning and few actually analyzed their current IT security to find out what really is required and most ideal to invest in.

The research will also show that some of the security threats are not being handled well, such as viruses, while others are better handled. The amount of security incidents are going down over the years, but the damage they cause is getting larger.

Keywords: IT security, investment, model, ROSI, network, management, administration.
Contents

1. Introduction .................................................................................................................. 1
   1.1 Overview ................................................................................................................. 1
   1.2 Purpose and problem at hand .................................................................................. 1
   1.3 Restrictions .............................................................................................................. 1
   1.4 Disposition .............................................................................................................. 2
   1.5 Method ..................................................................................................................... 2

2. Theory .......................................................................................................................... 3
   2.1 Threats ..................................................................................................................... 3
   2.1.1 Denial of Service .................................................................................................. 3
   2.1.2 Malicious Software ............................................................................................ 4
   2.1.3 SQL Injection ...................................................................................................... 5
   2.1.4 Unauthorized Access .......................................................................................... 5
   2.2 Economics in IT Security ......................................................................................... 6
   2.2.1 ROSI ...................................................................................................................... 6
   2.2.2 TCOS ..................................................................................................................... 6
   2.2.3 ALE ......................................................................................................................... 7
   2.2.4 Other methods ..................................................................................................... 7

3. Data / Surveys ............................................................................................................... 9
   3.1 Security Survey Results ........................................................................................... 9
   3.2 Own Survey and Interviews .................................................................................... 9
       3.2.1 Results of Own Survey and Interviews ............................................................... 10

4. Discussion of Security threats .................................................................................... 12
   4.1 Denial of Service .................................................................................................... 12
   4.2 Viruses ..................................................................................................................... 12
   4.3 SQL injection .......................................................................................................... 13
   4.4 Unauthorized Access ............................................................................................. 13

5. Analysis of Investment Models .................................................................................. 15
   5.1 ROSI ......................................................................................................................... 15
   5.2 TCOS ......................................................................................................................... 15
   5.3 ALE ........................................................................................................................... 16
6. Results................................................................................................................................. 18

   6.1 Overall conclusions ..................................................................................................... 18

   6.2 Further Work ............................................................................................................... 19

7. Works Cited.......................................................................................................................... 20
1. Introduction

This chapter will give an overview of the paper, explain the purpose and problem the thesis this report was built upon. The Restrictions, disposition and methodology are also explained to bring light on how the report is structured and how the work itself was done.

1.1 Overview

As the amount of types of security threats and amount of damage they can cause rises, less money is getting put in to IT security, especially because of the current economic recession. However, people and software with malicious intent take advantage of this and can cause even a greater amount of damage than what they usually would be able to do. As a result of this more money is spent recovering and restoring data from the security incidents than the amount it would have taken to prevent them, in a lot of cases (McAfee 2009).

There are many different threats to IT security, many of which have different counter-measures. Knowing what counter-measures to these threats are more effective than others is a big step of administrating networks and computers properly to make them secure. There are also models and algorithms which can suggest how much a company should invest into their IT security, what it can cost if they do not invest and how much they can save if they spend the specific amount. These models will be gone into more in depth, explained and analyzed to conclude which ones are the most optimal for different situations.

The end results will show that the smaller companies who were interviewed for the survey in this paper do not knowingly use any specific kind of model to analyze their security before investments; however they might use parts of them unknowingly.

1.2 Purpose and problem at hand

How much is the ideal amount that should be put into IT security, depending on company size, budget, and type of data being protected? As the actual amount may vary greatly, these models that can be used to calculate or estimate cost for security for all kinds of companies will all be explained more in depth later.

The main goal is to be able to answer these questions;
- How do these models estimate the optimal amount you need to invest into?
- Is there any model that is superior to the other ones and if so, why?
- Which way of calculating, if any, do companies use?

1.3 Restrictions

Since there is not enough time to look into every single model for security investments, not all of them will be analyzed, restrictions are made for the amount of how many of them will be looked into. The number of interviews for the survey is low because the information wanted for the type of survey made here is supposed to be qualitative instead of quantitative. This means that more time should be spent talking to the companies with the purpose of getting more detailed information.
1.4 Disposition
The rest of the paper is split into five more chapters. The second chapter is completely factual and theoretical about the threats and countermeasures of IT security, also the different investment models will be explained in that section. The third chapter is for different surveys and interviews within IT security and the results of them, including the one made for the sole purpose of this paper. The fourth chapter contains the discussion of the security threats and in the fifth chapter the actual analysis of the investment models will be presented. In the sixths and last content section the overall results of the whole thesis will be concluded and summarized.

1.5 Method
As the primary goals are to find an optimal way to see what investment model or models are theoretically most precise and ideal and what is used in practice when it comes to investing into IT security these methods need to be analyzed. Already existing articles and research papers about economics in IT security will also help the analysis and improve the accuracy of my own conclusions drawn from looking into them.

The surveys and interviews are used to see what threats are the main problems for companies and if the investment models they use actually are the most ideal to use based on how good their security is and if the right amount of the IT budget is being put into IT security.

The interviews were done by talking to the people responsible for IT investments within their companies on the phone and over email. As much relevant information as possible was attempted to be gathered from the large variety of companies interviewed, so that a good view over companies of different sizes in different areas all are included in the conclusions of this paper to make it as accurate as possible.

Security threats are analyzed using surveys for data to see the frequency of the security incidents, draw possible conclusions from the results by looking deeper into why these incidents occur even though there are strong counter-measures and find possible patterns.

The economic models are looked through after doing the interviews and used in examples to get a better understanding of what they actually calculate, how it is done and what can be concluded from the result of the different models. As the models are not all created for the exact same purpose it is not in every case easy to compare them since the result from the calculation is a different type. Because of that the models will also be analyzed by themselves more directly.
2. Theory

Planning, building and securing a network are not completely practical tasks, knowing what to invest in and how much to invest in it should be calculated. Calculating these things can save a lot of money from the perspective of investing just the right amount to secure the network, and not investing more than the value of the actual possible losses.

Knowing how attackers think and what tools and methods they can use to attack is also needed for knowing how to defend properly and effectively against them, which is why these threats will be explained in this section.

2.1 Threats

There are a great number of threats to IT security that can damage a company in many different ways. Protecting the integrity of data is an important thing to do for companies, great losses especially in a financial way can be had if there is a lack of counter-measures to the major risks and threats that are lurking on the internet looking for an unprotected opening that can be exploited and used to cause damage.

Of course not only the integrity of data needs to be protected, websites and similar services can also be attacked, overflowed with packets to slow these services down or even taken down by the immense amount of incoming data, have their vulnerabilities exploited sometimes even to the extent of damaging the hardware physically so that it needs to be replaced.

The most common problems and the most effective attacks will be explained in depth of what they are, how they are done and what you can do to prevent them (McAfee 2009).

2.1.1 Denial of Service

Although there are several different types of denial of service attacks they are all done for the same purpose. What the attack normally does is exploit the vulnerabilities of a Transmission Control Protocol/Internet Protocol (TCP/IP) connection and floods the targets connection queue. One of the ways to do it is to send the target more synchronization packets than it can handle attempting to make it unavailable to whatever users there are and that way disrupt the network components of the target (Microsoft 2003) (Pervasive Technology Labs 2001). There are however also types of denial of service which can target User Datagram Protocol (UDP) connections and flood the target with just UDP packets in order to make the device use all its system resources. These attacks are often referred to as UDP floods (IBM ISS 2010).

A similar method to the previously explained one is to send the target an overwhelming amount of ping packets, however to get this to work you need a much faster connection than the target you want to do this to (Pervasive Technology Labs 2001).

Permanent denial of service attacks are attacks that are so severe that they cause damage to the hardware, or damage the operating system so much that reinstallation is required. These types of denial of service attacks are done by exploiting some kind of security flaw in either the hardware or operating system and render it unusable so that it has to be replaced. PDoS as it is called is a type of attack that does not require a lot of resources, unlike the regular DoS attacks which can require whole bot nets for them to be able to work (Pervasive Technology Labs 2001).

As for counter measures for DoS attacks, firewalls can be used to deny some traffic and protocols; however it can not prevent any attacks on a web service since it will not be able to
distinguish the normal traffic from non-DoS traffic, as it all uses port 80 and blocking it would prevent anyone from accessing it.

Switches can detect and help prevent SYN flood DoS attacks using delayed binding, TCP splicing, deep packet inspection. Bogon filtering is also a switch feature which can prevent traffic from bad addresses (Pervasive Technology Labs 2001).

“Clean pipes” is a method used to separate bad traffic from non-DoS traffic. It makes all traffic pass through a proxy which contains a type of cleaning center software and only lets non-harmful traffic pass through to the target. This type of service can be provided by ISPs since central connectivity to the internet is needed. (Pervasive Technology Labs 2001) (DDoS Killer 2008).

The only thing that can help prevent permanent DoS attacks is to use tools to detect flaws, exploits and vulnerabilities in the hardware, however not much should have to be done as it is the responsibility of the company that created the hardware to secure their own products (Pervasive Technology Labs 2001).

2.1.2 Malicious Software
Malicious software can work in many different ways, they can corrupt or delete data, record keystrokes, spread themselves, interfere with the computers operation in an unwanted way and any combination of these. They can be categorized according to their functionality and behavior into different areas such as worms, trojans and root kits (Wikipedia 2010) (Microsoft Online Safety 2010).

A worm is a type of malware that is designed to replicate itself over and over and infect new computers as it does it without anyone having to do anything to it, unlike common viruses where human interaction is somewhat necessary for replication to go on. They spread quickly, sends copies of itself to email contacts and through the network. It can be act differently when it is on the computer, such as removing files, install a backdoor to create a zombie computer to be used for other type of attacks (Microsoft Security 2010) (VirusAll 2010).

A Trojan is a type of software that disguises itself as a non-harmful program, while it in reality can be malicious in many different ways. Trojans are often sent through email attachments or other full pieces of software to conceal them. When it is executed it silently runs hidden in the background and infects the system with i.e. a keystroke logger, file remover/modifier, making it part of a bot-net to perform DoS attacks (SANS Institute 2003).

Rootkits are designed to gain full control over the infected computer; they do this by exploiting security vulnerabilities. Rootkits can be used to replace operating system files to make it easier to install more malware and hide the processes the attacker has installed on the machine, that way the attacker can even gain access to hardware in the network such as a switch or router (ZSecurity 2010).

All types of malicious software basically have the same type of counter measures, everyday anti-virus, spyware, malware programs that are up to date are capable of taking care and protecting against all kinds of viruses. With the help of firewall software and an operating system with the most recent security updates it creates a very strong barrier against malware (Kaspersky 2010) (Microsoft Online Safety 2010).
2.1.3 SQL Injection
An SQL injection is an attacker altering and/or inserting new key words to a query with the intention to change the functionality of it. An attacker can have several different goals when doing an SQL injection attack, such as to extract data from a database since depending on what kind of database it is it could contain sensitive information which could hold some sort of value to the attacker. Performing denial of service is also a possibility with SQL injection attacks, this can be done by dropping (deleting) the database, or locking it, any way to make it unavailable to its users (William G.J. Halfond 2006).

The lack of input validation is the root of the SQL injection attacks, therefore defensive coding will prevent the majority of attacks against a database. Defensive coding is:

- Adding input type checking, to see what kind of SQL query is being entered to the database before executing it.
- Identification of the source of the query, checking the source of every input can prevent attackers from being able to do anything to the database, however this alone is not enough validation as it can be manipulated by an experienced attacker.
- Positive pattern matching is the practice of separating good input from bad input, if done right checking the queries for bad input can prevent unwanted actions quite well when combined with the other input validation methods (William G.J. Halfond 2006).

2.1.4 Unauthorized Access
Unauthorized Access is also one of the problems companies lose a lot of money to (Richardson 2008). Unauthorized access within network security is when an attacker somehow gets the information to i.e. an administrator or just a regular user account for a system and uses the access rights that account has to do things such as modify, gather, corrupt and distribute the data.

Having very easy passwords (also known as dictionary passwords) is one of the things that can make life easy for the attacker, as there are many tools and applications that can automatically go through and guess these without any problems (Computerhope 2010).

Preventing the majority of attempts to do unauthorized attacks is fairly simple and there are some things you can do to protect against which are free, maybe a bit obvious, but effective. Applying security update every time they get released is something that should be done, because there are always more flaws to be found in all kinds of software and operating system, and having these patched up will help.

Having good and complicated passwords will prevent the quickest ways to get unauthorized access. Changing passwords every few months, adding a password to the BIOS and not writing down passwords on notes and keeping them around the computer are the things you can do password wise.

Protecting the wireless network is also something that should be done; using the newer and stronger algorithms such as WPA2 for this can help against attackers nearby trying to get into the private company network, as you can extend and add many different extra types of authentication to it (Posey 2003).

Firewalls and the countermeasures for spyware are the last necessary protection, as the firewall prevents unauthorized incoming data which means that attackers will have a harder time being able to do anything to get access to the system (Computerhope 2010).
2.2 Economics in IT Security
Companies mindlessly investing into IT security could be a great waste of money by either investing too much so that it becomes a waste or when too little is invested it could put the virtual resources at great risk by leaving them exposed and unsecured. Therefore there are different financial models that can calculate what the optimal amount to invest into IT security is.

Some of the models calculate the same thing, but in different ways and some calculate something that others have not thought of calculating yet (e.g. models can calculate how much you can save by investing to protect the company’s assets or what it can cost you if attacks are successful etc). The purpose of this section however to only present these different types of models and explain them.

2.2.1 ROSI
Calculating the return of an investment is always an important thing to do in any kind of business, the idea of calculating the ROSI (Return On Security Investments) is very similar, however the variables which you calculate the ROSI from are harder to assign (Secure Business Quarterly 2001). According to the authors of “Return of security investments: A practical quantitative model”, there are five things the executives care about when a security investment is to be made, as quoted from their paper:

- How much is the lack of security costing the business?
- What impact is lack of security having on productivity?
- What impact would a catastrophic security breach have?
- What are the most cost-effective solutions?
- What impact will the solutions have on productivity? (Secure Business Quarterly 2001)

The way the return of security investment is calculated is:

\[ \text{ROSI} = \frac{(\text{Cost of Risk Exposure} \times \text{Percentage of risk mitigated}) - \text{Cost of security investment}}{\text{Cost of security investment}} \]

This way it will decide if the investment is financially worth it, or if it is not. If the cost of the security investment is greater than the cost of the actual risk of the exposure, then it is obviously not a good investment to do (Secure Business Quarterly 2001). The result of this calculation is a percentage, which shows how big the return of the security investment is, an example is shown in the analysis section.

The ROSI is one of the most complex calculations to do within economics in IT security; it even includes another method and uses it to be even more precise, the annualized loss expectancy (ALE) which is explained further in another subsection (Secure Business Quarterly 2001).

2.2.2 TCOS
Another method of calculating is called “the total cost of security”, it has been claimed by the authors that it has many advantages over the previous ways of doing it, as the other methods are too confusing and misleading in my different ways. The main advantages are claimed to be:

- It is compatible with enterprise risk management frameworks, generally accepted accounting practices, enterprise resource planning packages and “economic theories of the firm and rational decision making with uncertain and incomplete information”. 

• Giving an overall good framework for integrating different security metrics into an “economically meaningful composite measure”.
• Less data collection required.
• From a theoretical aspect the framework of this method seems usable for many different kinds of companies as it has a very wide range of risk profiles to satisfy many kinds of different needs [6].

Explained in the authors’ own words, the way it is calculated is;

• \( \text{TCoS} = B + SI + C \), where:
  • \( \text{TCoS} \) is the Total Cost of Security risk measure
  • \( B \) is the budgeted security costs and losses for the period (i.e. median costs, or within a margin of the median),
  • \( SI \) is the self-insurance premiums to cover low probability-high impact losses, and
  • \( C \) is the costs of business continuity to cover deal with catastrophic scenarios, allocated according to information security causes and effects (Thomas 2009).

2.2.3 ALE

Annual Loss Expectancy (ALE) is a way to calculate the losses that can be expected due to security risks. It is calculated by taking the single loss expectancy times the annual rate of occurrence. The annual rate of occurrence describes the amount of times you can expect a risk to happen over a full year. The single loss expectancy is the cost for a single risk to actually go through (Huaqiang Wei 2001) (Risky Thinking 2010).

The ALE is a four step process where you:
1. Identify your assets and assign current values them.
2. Identify the risks and what the actual vulnerabilities are.
3. Calculate ALE.
4. Find what counter measures are worth investing in and how much they would reduce the current security risks for the assets (Huaqiang Wei 2001).

More specifically you calculate the loss expectancy for the assets in the following way:

\[
\text{Single Loss Expectancy (SLE) = Exposure Factor (EF) * Asset Value (AV)}
\]

\[
\text{Annual Loss Expectancy (ALE) = SLE * Annual Rate of Occurrence (ARO)}
\]

The ALE is a smaller and a more simple method compared to some of the other ones, such as the return of security investment.

2.2.4 Other methods.

There are of course a lot of other methods which also mostly calculate different things, specific models for smaller parts of the network, things like analysis models for network intrusion detection systems [7]. There are also extremely advanced models which require more than just basic math and network security administration knowledge to understand (Huseyin Cavusoglu 2004).

Many models however are very simple, to help out smaller companies so that they can do the calculations on their own. In example for some companies, estimating things like the full potential loss of what an attack would do could work, but since for many organizations that number could be many millions it is not an ideal way to do it. However it can be a good starting point for
calculating the investment that needs to be made for a lot of smaller companies that do not have the resources to do a complete and complex analysis to calculate the perfect amount (Huseyin Cavusoglu 2004).
3. Data / Surveys
The data collected and used for this research was collected by a variety of companies and people but with similar goals for the use of the data. The data presented are the main points relevant to this particular paper while the less interesting parts are left out and not summarized.

3.1 Security Survey Results
AllCovered Security Survey
In the survey by AllCovered they ask smaller businesses with different sizes what types of IT security software and devices they have. Close to every company stated that they have firewall, anti-virus software, spyware protection and spam control, however most did not have smart password policy, automatic patch management and no network policies either. The survey was done in 2006 so the data is a tiny bit outdated but still somewhat relevant (AllCovered 2006).

Companies thought they had secure networks for the most part but over 50% in average had virus problems. A minor part also had attackers targeting them and attacking, unauthorized access and lost backups. The major thing about what is worth taking notice to in the survey is that only an extremely small amount of companies had no security problems whatsoever, less than 5% (AllCovered 2006).

McAfee: The Security Paradox
McAfee’s survey shows that the majority of “midsized” organizations (500 employees or less) are seeing more and more security incidents compared to the year before the survey was made (2009). Another major thing it shows is that companies decide to spend less money on IT security mainly because of the economic recession and the cybercriminals use the opportunity of this to be more offensive and pose greater threats.

McAfee also claims that these midsized organizations are being targeted more than organizations which are larger (500 or more employees) and they should not feel as safe as they think they are, it will hurt them more than it will help (McAfee 2009).

CSI Computer Crime & Security Survey
The CSI survey is the largest, most thorough and has a large variety of respondents. The findings of the survey show that companies lose a lot of money however the sizes if the companies are not mentioned so it is hard to hard to draw conclusions from some of the information. It shows in detail what security threats have been most common, and the results from the previous years as well so that it is easy to see how the different threats have changed.

Almost every type of security threat has gone down in occurrence compared to the previous years. From 1999 to 2008 virus rate of occurrence has gone down from 90% to 50% and it could be safely assumed that it will go down even more over the years to come. Overall the rate of cybercrime seems to be getting smaller and organizations start to find better ways to protect themselves with the technology at hand.

3.2 Own Survey and Interviews
As an additional source of information on how companies invest into IT security my own interview will cover the aspects missing related to this paper and which are also not covered in the other surveys made by others. The main points my survey is supposed to show are the specific economy related issues companies are having and also to see and how smaller companies (20-100
employees) handle their IT security compared to the ones in the other surveys. The companies participating are from all kinds of areas of expertise to get a diverse and not a one-sided survey, so that it covers not only one type of company, but instead the majority of them.

The surveys were done mainly over phone, but also over email if the company did not feel the need or desire to talk over the phone about the questions that were asked. The main topics discussed with the companies which were participating in the surveys when doing the interviews were:

- Number of employees at the company
- Yearly revenue/turnover
- How investments towards IT security were planned, hinting towards if they actually tried to follow some kind of model when investing, i.e. if some type of security analysis was done.
- What they thought their weakest point of their network was or what the biggest threat towards them is.
- Cost of IT security related investments per year.
- Recent IT security related incidents, how it was dealt with, if anything changed after them.
- If they have any recent and/or upcoming IT security related investments, if so, what they are and why they are being made.

The names of the companies participating in the survey are not given out to protect them from potential targeted attackers who after skimming through this would know their levels of security and vulnerability.

3.2.1 Results of Own Survey and Interviews

Out of the companies that participated in the survey about half of them claimed they did some kind of research or security analysis before investments. However an equal amount of companies which did security analysis and the ones who did not have had several security incidents recently.

The majority of the companies claimed that they had no weak points in their IT security structure. The ones that thought they did said the most major problem is the human factor; bad at handling passwords, downloading malicious software by mistake and problems with stolen computers.

The amount of total budget invested into IT security varied greatly for the companies even though they were somewhat similar size; there are companies investing large amounts and who are still having security problems and there are some companies investing smaller amounts who have had no problems whatsoever. From the results, it looks completely random for which companies have security problems and which ones do not.

Type of company does not seem to play any role either, there are some who work a lot with computers and have sensitive data to protect, but do not have any problem. At the same time there are some who do not work with sensitive data at all, but have had attacks directed against them.

The most common attacks against these companies were virus problems and attacks against web servers or other kinds of web services. The ones that had incidents did not change or make their upcoming investments larger, and the ones that had none still sometimes thought investing more still seemed necessary. Some companies interviewed for this survey gave the impression of
that they do not always take IT security as a serious issue and they do not always realize what could be lost if something goes terribly wrong.
4. Discussion of Security threats

The security threats, which are the main ones to companies of most sizes these days (Richardson 2008) are discussed in this section with the help of the data collected and summarized in the previous section, and also with the help of several articles related to their subjects.

4.1 Denial of Service

Denial of service, very likely the strongest attack possible on a web service as it is the hardest one to prevent considering what kind of counter-measures there are for it. There being so many different types of denial of service attacks, and so many tools to modify the details of them also adds more complexity to defending against it.

It comes to no surprise that denial of service is one of the main security incidents companies have problems with (Richardson 2008). Some security companies have been working and sometimes collaborating together on the issue of trying to find the best way to protect against the DoS attacks and it seems the strongest solution that they have worked out is the Clean Pipes model explained in the section of security threats and counter-measures (Arbor Networks 2010).

If a company has been experiencing DoS attacks, has had trouble to protect against them themselves and are losing money due to the fact that their services are made unavailable, there is no logical reason to not have some kind of Clean Pipes service for the data directed to the company. Having that threat taken care of, a company should be able to feel much safer IT security wise.

There have been companies in the past that had to shut down because of a few people or in some cases just one person not wanting them to exist, especially anti-spam and security companies, that person being an attacker or spammer who have the resources to do very effective distributed DoS attacks on the company, their web services and their customers. To smaller companies who absolutely have to use the internet and IT this can be quite a threat if they do not have the resources it takes to prevent them (Kitching 2008).

4.2 Viruses

Viruses have always been the main security problem that most companies have and most companies lose most money too, IT security wise (Richardson 2008). The question is why this is, with so many antivirus software types, anti-spyware, firewalls. Even though computer virus incidents have gone down by a lot the past years, the numbers of them still seems too high considering all the effective counter-measures.

Considering that there are only extremely few companies without proper firewalls and antivirus software installed on their computers (AllCovered 2006) (Richardson 2008), there are several likely scenarios which could explain the amount of virus problems that companies are having and have been having.

One of the scenarios is that people working at a company either take laptops from work with themselves when they go home, to have a possibility to work from there or taking their own personal laptop with them to work and connecting it to the network. The problem here would be that a personal home network is very likely less secure than a company’s network and the computers are not maintained and software kept up to date by an IT administrator, which means that there is a greater chance of malicious software floating around on the home computers and
have it easier to get through the network because it would not be preventing the viruses from doing what they should not be allowed to do.

Another possibility why viruses cause companies to lose money on them is that the network and connected devices are not being maintained properly, some missing anti malware software, being un-updated and missing the latest security updates from their operating systems.

There is also a likely scenario where the anti-virus software and/or operating system are just flawed, not good enough and do not prevent all these viruses from getting through. Looking at statistics there does seem to be quite a bit of flaws and weak anti-virus software (SurfRight 2009). The defensive layers that anti-viruses are supposed to give do not seem to counter as much as they should, especially when they are not kept up-to-date and in combination with a weaker operating system security wise there seems to be a great lack of malware detection. However taking into account that companies should be more organized and have more knowledge within IT security the numbers of virus problems should not be that high, however the amount of infections have been decreasing steadily the past years which shows that it is slowly getting more secure and safe over time (AliCovered 2006) (McAfee 2009) (Richardson 2008).

4.3 SQL injection
SQL injection is a completely targeted attack done by an attacker that is trying to, or already has found a flaw in i.e. a web application. Most of the counter-measures to SQL injection attacks are fairly simple but can cost a lot if they are forgotten about and ignored, making the attacks so much easier for the person trying to cause damage.

Never trusting user input, limiting access to user accounts and encrypting or hashing passwords are such effective counter-measures and take up little time to implement compared to recovering lost data after the attack.

SQL injections were for quite a while not that big of a threat but have become more popular and it has over the years become an interesting way of attacking over the internet as the amount of usage of web applications has been rising. Apparently there is not a single counter measure that alone can prevent all SQL injection attacks, but filling up all the security flaws with different techniques is an effective way to secure the web applications (Warneck 2007).

4.4 Unauthorized Access
There are a lot of possibilities to enhance the security to stop unauthorized access. Using strong algorithms like WPA, instead of the weaker ones like WEP for wireless networks (Posey 2003). Every extra counter measure against unauthorized access adds another layer that an attacker has to get through to before he can do what he wants.

Properly setting up and maintaining the authorization mechanisms for a company seems to be something that is more problematic, but however it is something that is slowly being dealt with over time. The amount of successful unauthorized access attacks seem to be going down slowly over time which either means companies are taking it more seriously and its getting easier to handle with the amount of available tools which is a good thing (Richardson 2008).

For bigger companies and organizations managing and maintaining an authorization system takes times, using active directory and managing it takes on average 5.8 hours per 1000 users. Most companies manage systems like this manually, only very few use an automatic solution. With
thousands of employees, even a low turnover rate will create a lot of work for the person managing the system and errors are bound to happen at some points (Imanami 2008).

Unless something special happens with the development of authorizations mechanisms, it is very likely that there will always be some unauthorized access attacks, at least for quite some time into the future, however it should be possible without much effort to lower the amounts.
5. Analysis of Investment Models
The analysis performed on the investment models was done as the last thing in this research, because as much knowledge as possible on the subject was required and wanted so that there was enough ability to be as accurate as possible, so that the majority of mistakes and inaccuracies could be avoided.

5.1 ROSI
At a first glance the way to calculate the return of security investments might seem like a simple formula, however after going through it, it looks like a calculation that should not be attempted by someone who is not fully aware of what work it requires as it will only hurt more than it helps if done wrong. There seems to be quite some work and precision required to be able to complete a full ROSI calculation.

It seems as the ROSI model is mainly made for and perfected for most types of companies with all types of sizes, there are possibilities to adjust it and you are supposed to be able to apply it to different types of company environments. It looks like it would be a lot of work no matter how much it gets adjusted, which makes it seem less ideal for smaller companies, if you choose to dumb it down and make it simpler there are other methods and solutions that are likely to be more ideal and helpful.

Calculating the return of an investment has been around for a long time, including the one for IT security, it should not as to a surprise that this method has been worked on and perfected over the years, as well as used by many companies. What also is noteworthy is that there is more than one way for calculating this and the equation can differ a bit, however the idea stays the same.

Example of ROSI:
A company is a target of an attack and estimate the total recovery and productivity cost of it to 20000. Attacks like that are expected to happen four times a year according to the company and they decide to implement a counter measures for it which costs 20000. The counter measure is estimated to prevent 75% of all attacks, so in this case it will stop three attacks. The ROSI calculation can now be done with the variables like this:

- Risk exposure: 20000 per exposure, with four exposures a year = 80000.
- Percent of risk mitigated: 75% of all attacks.
- Cost of security investment: 20000.
- Return of security investment: \[
\frac{(80000 \times 0.75) - 20000}{20000} = 200\%
\]

We can see that the return of security for the investment is 200%, however there are a lot of assumptions made as it is hard to exactly estimate how many attacks there are going to be and how much they are going to cost. Let us say three attacks that were blocked would have cost 10000 each and a fourth attack which would have gone through could cost 50000. It would still be an average of 20000 per attack, but do so much damage that a stronger security solution would have been better (ISACA 2010).

5.2 TCOS
Authors of the method seem to imply that the model still needs more research and verification to make sure it would work and at the same time they claim that all the other method have “has
severe or fatal limitations when applied to information security risk”, however this one is different (Thomas 2009).

The variables for the TCoS are supposed to be bigger pieces instead of small estimated numbers and this way it will be more reliable. However this means that even more has to be estimated and calculated before the final number comes out. It is an interesting approach as from my point of view it could really go both ways depending on how much time is spent, if it is done sloppily or precise and either it would work really well, or not well at all.

What also is noteworthy is that no real way to calculate the different “pieces” (variables) has been given. After looking over it more the method seems a little bit vaguer every time, but at the same time it does seem to have a lot of potential once the current problems with it get figured out and adjusted. The main issue seems to be that it is not matured enough and it has not been practically tested as much as the other methods, considering return of security investments is based on Return of Investment (also known as Rate of Return, Rate of Profit), which is a financial model which has been around even longer.

Example:
The badly defined variables make the result of an example calculation harder to process than it would have been if they had been better and more precise. Let us say a company estimates the variables to calculate their budgeted security costs to be 200000, the self insurance premiums which are meant to cover the high impact losses to 30000 and at last the preparations for catastrophic scenarios to 20000.

This means that the variables are defined so that $B = 100000$, $SI = 30000$ and $C = 20000$, which can be calculated to:

$$TCoS = B + SI + C = 150000$$

It does not take much to see that estimations like these in this model are imprecise and that other methods which are not in the phase that this one is in will be more reliable. The framework overall does seem like a different approach to the whole issue and it could be interesting to see what the actual end result will be when it is completed.

5.3 ALE
Annual loss expectancy is less to calculate and estimate but however it gives another result when it is used. One of the most important things to remember is to include all the associated asset values, an inexact calculation is likely to do more harm than good.

ALE has been around long enough and accepted so much that there are multiple programs to help out and make the calculation of ALE easier (Computerhope 2010). Identifying the threats is also a part of this model and also estimating how often they will occur, since that is the way the single loss expectancy is calculated.

What easily can be noticed is that there always is loss expectancy no matter what you do and what numbers you use for the calculation. However this is pretty obvious as it makes sense, except for that at one point it will not be worth investing more to protect the asset.

Example:
Let us say that there is a database where the data stored on it is valued at 50000, which has a risk exposure factor of 0.6. By calculating the product from those two values the single loss
expectancy will come out at 30000. Estimating the annual frequency of an attack against the database at 0.15 the annual loss expectancy for that specific asset will be 4500.

Calculated from the start using the variables in the formula the Asset Value = 50000 and Exposure factor = 0.6, this means that the Single Loss Expectancy = \( AV \times EF = 30000 \). Now using the Annual Rate of Occurrence = 0.15 (15%) and Single Loss Expectancy it can be calculated together like this:

Annual Loss Expectancy = \( SLE \times ARO = 4500 \).

That means that the expected loss for the asset is 4500 a year on average with the current security levels.
6. Results

The results concluded in this section mainly are the ones which are related to the questions asked for which the paper was made, but also the results of the subjects the research directly came in contact with.

6.1 Overall conclusions

So these models, how exactly do they calculate things? In every model there is always some amount of estimating that needs to be done. In a lot of models the majority of the variables for the calculation are estimated values. The more variables are estimated or made up, the less accuracy the result will be. This is the biggest problem with almost every single model. However that is the way it has to be and just because the number that comes out is not precise it will give some idea of how much could be lost and what should be thought about when the company invests more into IT security.

The main ingredients for the different calculations vary a little from model to model, but since they all strive to accomplish similar goals, the thing that seems common in for most models is to calculate what would happen if no investment is done. It does not have to be the end result of the calculation, but it always seems to be a factor of what the end result becomes.

It is hard to say if there really is a security risk calculation model which is better than others, since different things are calculated. However, the model that by far sticks out, has been around a very long time and has been worked on for perfection is the ROSI which also contains the ALE.

The newer more recent models have some good and original ideas which need to be adjusted and studied more before they can become as solid as the older ones. Once that happens once that happens there will undoubtedly be some interesting changes to this area. A greater variation of models will give a better and more precise insight to the investing into IT security subject.

The people responsible for IT security investments in their companies interviewed for this paper were not in all cases as knowledgeable as expected. Several of them had no actual idea that things like models for risk calculation actually existed. The other ones who analyzed their security did not follow any specific model - knowingly that is - however it is likely that when they did their security analysis they actually did parts of some model without knowing it.

Another thing that could be concluded from the survey is that there is only a small or no difference between the companies of smaller size who actually do security analysis and ones who do not. However since it was not a quantitative survey it is not exactly that accurate, but should not be completely ignored.

A lot of the security threats that cause a lot of problems, more than they should. Viruses and SQL injection attacks are the two main threats which should not be any problems. Companies really need to maintain the simple things better; setting a policy for having good, up-to-date anti-virus software on every computer attempting to connect to the network is pretty important, easy to manage and at the same time saves a lot of potential trouble. Other attacks are harder to prevent, but in a most cases have to be targeted attacks performed manually by the attacker, such as denial of service. Overall, since most of the threats and the amount of how many companies have problems with them have been going down, it means that they are slowly starting to realize what needs to be done in order to protect themselves from the threats. At the same time there is a lot of room for improvement which hopefully will be seen over time.
6.2 Further Work
Some questions were answered and some were not, and at the same time several new questions have come up. New possible lines of work which can be explored have arisen as a result of this.

- Quantitative survey for larger companies and their investment strategies to see how they handle investments and straight up ask if they follow any specific models when analyzing their security.
- More thoroughly investigating in the security threats and which types of companies has the most problems, more specifically how and if investment strategies affect it.
- Interview IT security consult companies to find out what methods they use.
- Research why some of the security threats are such a problem when there are really effective counter measures.
7. Works Cited


