Accessing a web based business system through a smartphone, a risk analysis

av

Anton Nilsson

LIU-IDA/LITH-EX-A--15/009--SE

2015-03-03
Final thesis

Accessing a web based business system through a smartphone, a risk analysis

av

Anton Nilsson

LIU-IDA/LITH-EX-A--15/009--SE

2015-03-03

Handledare: Juha Takkinen
Examinator: Nahid Shahmehri
Abstract
This thesis project has been performed at (and for) a company named Strödata. The purpose of the project has been to perform a risk analysis on Strödata’s web based business system, and specifically analyze how access to the business system through smartphones would affect the risks posed to the system. This has been done to help decide if smartphone access should be enabled. An implementation of a web application which is suited for use on a smartphone has also been developed, as a proof-of-concept, to grant access to a limited part of the business system. The method used to perform the risk analysis has been CORAS, as presented by Braber et al in [1]. CORAS is a risk analysis method designed with IT-systems specifically in mind. The method is divided into seven steps. The new web application is an ASP.NET MVC3 site that uses JavaScript, jQuery and Ajax-JSON.

The risk analysis showed, among other things, that the benefits of enabling smartphone access to the business system are larger than the risks it introduces. Smartphone access also opens up many new possibilities to implement interesting new features or improve old ones. The risk analysis also showed that there are risks to the system that need to be dealt with. For these, risks treatments were identified to lessen their probabilities and/or their consequences should they occur. Some treatments were completely successful in eliminating the risks they treat, others were not. However, the treatments that were not completely successful did reduce the risks far enough that perhaps they should be re-evaluated as un-/acceptable.

The conclusions that can be drawn from this thesis project are that although enabling smartphone access to the business system introduces new risks to the system, the access also reduces certain risks. How costly the new risks are and how much the access reduces risks varies from company to company and from system to system. For Strödata, the reduction to certain risks was large enough to outweigh the new risks that would be introduced. Regarding the possibility to implement smartphone access to the business system, it is possible using more modern technologies, methods and frameworks; such as those mentioned above.
## Table of Contents

Abstract ......................................................................................................................... ii

Figure and table register .............................................................................................. v
  Figures .................................................................................................................. v
  Tables .................................................................................................................. vi

Glossary ......................................................................................................................... viii

Risk analysis .............................................................................................................. viii
  General ............................................................................................................... ix

1 Introduction .......................................................................................................... 1

2 Background & Theory ....................................................................................... 3

3 Risk analysis ......................................................................................................... 17
  3.1 Introduction .................................................................................................... 19
  3.2 High-level analysis ...................................................................................... 20
  3.3 Approval ....................................................................................................... 26
  3.4 Risk identification ....................................................................................... 32
  3.5 Risk estimation ............................................................................................ 35
  3.6 Risk evaluation ............................................................................................. 40
  3.7 Risk Treatment ............................................................................................ 44

4 Analysis ................................................................................................................. 53
  4.1 Accessing the business system from a smartphone .................................. 53
  4.2 Resulting system view ................................................................................ 58
  4.3 What did the risk analysis show? ............................................................... 65

5 The Application .................................................................................................... 68
  5.1 Suggested solutions .................................................................................... 68
    5.1.1 Adapted WebApp GUI 1 ..................................................................... 69
    5.1.2 Adapted WebApp GUI 2 ..................................................................... 69
    5.1.3 Rebuild 1 ............................................................................................. 69
    5.1.4 Rebuild 2 ............................................................................................. 70
    5.1.5 Rebuild 3 ............................................................................................. 70
  5.2 New application use case ............................................................................. 70
  5.3 Development ................................................................................................. 71
  5.4 Demonstration ............................................................................................... 76

6 Discussion and conclusions ............................................................................... 78

References ................................................................................................................. 83
Figure and table register

Figures
Figure 2.1 Use cases for Strödata’s web based business system .................................................. 4
Figure 3.1 Direct asset .................................................................................................................. 19
Figure 3.2 Indirect asset .............................................................................................................. 19
Figure 3.3 Risk ........................................................................................................................... 19
Figure 3.4 Unwanted incident ................................................................................................. 19
Figure 3.5 Stakeholder .............................................................................................................. 19
Figure 3.6 Vulnerability ............................................................................................................. 19
Figure 3.7 Non-human threat ................................................................................................... 19
Figure 3.8 Unintentional human threat .................................................................................... 19
Figure 3.9 Intentional human threat ......................................................................................... 19
Figure 3.10 Treatment ............................................................................................................... 19
Figure 3.11 System overview .................................................................................................... 19
Figure 3.12 Class diagram showing a conceptual view of the target ........................................... 21
Figure 3.13 Collaboration diagram illustrating physical communication lines ........................ 21
Figure 3.14 Sequence diagram for the “Reporting work” task .................................................. 22
Figure 3.15 Initial asset diagram .............................................................................................. 23
Figure 3.16 Initial threat diagram for intentional human threats ................................................. 25
Figure 3.17 Initial threat diagram for unintentional human threats ........................................... 26
Figure 3.18 Initial threat diagram for non-human threats ........................................................ 26
Figure 3.19 Asset diagram ......................................................................................................... 28
Figure 3.20 Threat diagram for intentional human threats ......................................................... 33
Figure 3.21 Threat diagram for unintentional human threats .................................................... 34
Figure 3.22 Threat diagram for non-human threats .................................................................... 35
Figure 3.23 Risk estimation diagram for intentional human threats ........................................... 36
Figure 3.24 Risk estimation diagram for unintentional human threats ..................................... 37
Figure 3.25 Risk estimation diagram for non-human threats .................................................... 39
Figure 3.26 Risk diagram for the “Customer information”-asset ................................................ 42
Figure 3.27 Risk diagram for the “Company information”-asset ................................................ 43
Figure 3.28 Risk diagram for the “WebApp”-asset ..................................................................... 43
Figure 3.29 Risk diagram for the “Physical server”-asset .......................................................... 44
Figure 3.30 Risk diagram for the “Financial information”-asset .............................................. 44
Figure 3.31 Risk treatment diagram for intentional human threats ......................................... 45
Figure 3.32 Risk treatment diagram for unintentional human threats ...................................... 47
Figure 3.33 Risk treatment diagram for non-human threats ..................................................... 49
Figure 3.34 Treatment overview diagram for the “Customer information”-asset ...................... 50
Figure 3.35 Treatment overview diagram for the “Company information”-asset ...................... 50
Figure 3.36 Treatment overview diagram for the “Financial information”-asset ...................... 51
Figure 3.37 Treatment overview diagram for the “WebApp”-asset ........................................... 51
Figure 3.38 Treatment overview diagram for the “Physical server”-asset ................................. 52
Figure 4.1 Tele2 coverage map ................................................................................................. 54
Figure 4.2 Telenor coverage map ............................................................................................. 54
Figure 4.3 Telia coverage map .................................................................................................. 54
Tables
Table 1 Risk analysis glossary .............................................................................................................. viii
Table 2 General glossary ....................................................................................................................... ix
Table 3 Risks [9] discussed in Smartphone security: Information security risks, opportunities and recommendations for users. ....................................................................................................................... 9
Table 4 Description of usage scenario levels [9]. .................................................................................. 10
Table 5 CORAS-icons. Source: http://coras.sourceforge.net/downloads.html ................................... 19
Table 6 Initial asset descriptions .......................................................................................................... 22
Table 7 Initial high-level threat table .................................................................................................. 24
Table 8 Asset descriptions .................................................................................................................... 28
Table 9 Asset rankings .......................................................................................................................... 29
Table 10 Likelihood scale ..................................................................................................................... 29
Table 11 Consequence table for the "Customer information"-asset ...................................................... 30
Table 12 Consequence scale for the "Company information"-asset ...................................................... 30
Table 13 Consequence scale for the "Physical server"-asset .................................................................. 30
Table 14 Consequence scale for the "WebApp"-asset .......................................................................... 31
Table 15 Risk evaluation matrix for the "Customer information", "Company information", "Physical server" and "WebApp" assets .............................................................................................................. 31
Table 16 Consequence scale for the "Financial information"-asset .................................................... 31
Table 17 Risk evaluation matrix for the "Financial information"-asset ................................................ 32
Table 18 Combined likelihood table for unwanted incident: CC1 ..................................................... 36
Table 19 Combined likelihood table for threat scenarios "The WebApp goes down" and "The database crashes" ........................................................................................................................................... 37
Table 20 Combined likelihood table for unwanted incident: CA2 ..................................................... 38
Table 21 Combined likelihood table for unwanted incident: CI2 ..................................................... 38
Table 22 Combined likelihood table for unwanted incident: CA4 ..................................................... 39
Table 23 Combined likelihood table for unwanted incident: CA5 ..................................................... 40
Table 24 Risk evaluation matrix for the "Customer information"-asset ................................................ 40
Table 25 Risk evaluation matrix for the "Company information"-asset ................................................. 41
Table 26 Risk evaluation matrix for the "WebApp"-asset ......................................................................................... 41
Table 27 Risk evaluation matrix for the "Physical server"-asset ................................................................................. 41
Table 28 Risk evaluation matrix for the "Financial information"-asset ................................................................. 41
Table 29 Consequence changes for the "Financial information"-asset and intentional threats ...................... 60
Table 30 Likelihood changes for threat scenarios for unintentional threats ...................................................... 61
Table 31 Likelihood changes for unwanted incidents for unintentional threats .............................................. 62
Table 32 Likelihood changes for threat scenarios for non-human threats ......................................................... 63
Table 33 Likelihood changes for unwanted incidents for non-human threats .................................................. 63
Table 34 Resulting risk evaluation matrix for the "Customer information"-asset ............................................. 63
Table 35 Resulting risk evaluation matrix for the "Company information"-asset ............................................. 64
Table 36 Resulting risk evaluation matrix for the "WebApp"-asset ........................................................................ 64
Table 37 Resulting risk evaluation matrix for the "Physical server"-asset ......................................................... 64
Table 38 Resulting risk evaluation matrix for the "Financial information"-asset ............................................. 64
Table 39 Risk evaluation matrix for the "Financial information"-asset ............................................................... 64
Table 40 Changes in calculated losses with and without treatments ................................................................. 65
Table 41 Input constraints for the work report form ......................................................................................... 75
## Glossary

### Risk analysis

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>An asset is something in or related to the target to which the client assigns great value [1].</td>
</tr>
<tr>
<td>Client</td>
<td>The Company, organization or other that has requested the risk analysis.</td>
</tr>
<tr>
<td>Direct asset</td>
<td>A direct asset is an asset that may be harmed directly by an unwanted incident [1].</td>
</tr>
<tr>
<td>Indirect assets</td>
<td>An indirect asset is an asset that may only be harmed if direct assets are harmed first [1].</td>
</tr>
<tr>
<td>Intentional threat</td>
<td>Intentional threats are threats that intentionally causes harm to a system, for example: a disgruntled employee.</td>
</tr>
<tr>
<td>Non-human threat</td>
<td>Non-human threats are threats that cannot be controlled. Non-human threats may be power failures or earthquakes etc.</td>
</tr>
<tr>
<td>Risk</td>
<td>A risk is a combination of threat, threat scenario, unwanted incident and a corresponding asset. A risk is described as the probability that an unwanted incident occurs combined with the consequences a threat would have for the assets if it does occur (calculated as: Probability * Consequence value = Risk)</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>A stakeholder is a person, a group, an organization or a company who has an interest in the target.</td>
</tr>
<tr>
<td>Target</td>
<td>The target is the system on which the risk analysis is to be performed.</td>
</tr>
<tr>
<td>Threat</td>
<td>A threat is a potential cause of an unwanted incident, such as a disgruntled employee or an earthquake.</td>
</tr>
<tr>
<td>Threat scenario</td>
<td>A threat scenario is a situation where a threat causes one or more unwanted incident(s).</td>
</tr>
<tr>
<td>Treatment</td>
<td>A treatment is a way to reduce the probability of a risk occurring and/or the following consequences. A treatment could be a way to remove a vulnerability (for example: through further education/training of the users) or a mechanism to reduce the impact an unwanted incident would have (for example: regular backups of important data).</td>
</tr>
<tr>
<td>Unintentional threat</td>
<td>Unintentional threats are threats that do not intend to harm the system but that may do so by accident or due to carelessness etc. For example: a sloppy employee.</td>
</tr>
<tr>
<td>Unwanted incident</td>
<td>An undesired incident caused by one or more threat scenarios. The unwanted incident affects one or more assets in a negative way. For example: Compromises the confidentiality of the information in the database.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Vulnerabilities are weaknesses in the system that can be exploited by one or more threats.</td>
</tr>
</tbody>
</table>

*Table 1 Risk analysis glossary*
### General

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>In this report availability refers to a property of information. The availability of the information refers to the accessibility of the information (can the information be accessed or not).</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device, refers to employees bringing their own devices, with their own data and applications, into the workplace.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>In this report confidentiality refers to a property of information. That information is confidential means that it is not publicly known, only authorized people are allowed access to the information.</td>
</tr>
<tr>
<td>ENISA</td>
<td>Abbreviation for European Network and Information Security Agency.</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission.</td>
</tr>
<tr>
<td>Integrity</td>
<td>In this report integrity refers to a property of information. If the integrity of the information has been compromised that means that the information may not be correct.</td>
</tr>
<tr>
<td>WebApp</td>
<td>Strödata’s business systems web application is referred to as “WebApp” in this report.</td>
</tr>
<tr>
<td>Webview</td>
<td>In this report “webview” refers to an Android view that displays web pages.</td>
</tr>
<tr>
<td>Sunshine scenario</td>
<td>The simplest use case scenario, where everything is performed correctly.</td>
</tr>
</tbody>
</table>

Table 2 General glossary
1 Introduction

The world is getting more mobile every day, everyone and everything is affected. The possibilities that mobile devices provide are endless and most of us keep the devices with us everywhere we go. Strödata is a company that provides IT-services, they supply their customers with everything from servers and printers to software and support. The company is based in Skåne with offices in Vinslöv and Trelleborg. There are eight people employed at Strödata at the time of writing. Today Strödata utilizes a web based business system which fills most of their needs. Being web based, the system is already rather mobile. The system has been in use since 2004 with various updates applied since it was deployed. In the interest of mobility, both in their own company as well as others, Strödata feels that the next logical step towards further mobility is to access the business system from smartphones. At the time of writing the system is not adapted for this, when the system was developed there were no smartphones available. Since the system deals with Strödata’s information about customers, products, billing etc, the security of that information is a large concern. All parts of the CIA trinity (Confidentiality, Integrity & Availability) need to be taken into consideration. To find out how accessing the business system through a smartphone could affect the risks posed to the system, a risk analysis has been conducted. First, on the system as it is today (see section 3), and second to determine how the smartphone access would affect the risks that were identified in the first analysis (see section 4). The results from the analysis helps to determine if access to the system from a smartphone should be enabled. Two interesting points to consider regarding how the risks posed to the system would be affected by enabling smartphone access are:

- What new risks, if any, will the smartphone access cause?
- Could the smartphone access decrease or even completely remove any existing risks?

The method that has been used for the risk analysis is CORAS as presented by Braber et al in [1]. CORAS will be further presented in section 3 of this report. A simple way to explain CORAS is as a model for risk analysis with seven steps:

1. Introduction
2. High level analysis
3. Approval
4. Risk identification
5. Risk estimation
6. Risk evaluation
7. Risk treatment

This report also contains a section where the resulting system view (where all the suggested treatments have been implemented) is presented and compared to the system view without any treatments implemented. See section 4.2.

Since the system in its current state is not a viable option for smartphone access, part of this project has been to implement a proof-of-concept web application where smartphone access to a limited part of the business systems’ features is possible. The part of the business system that the proof-of-concept web application implements is the work reporting feature. The new web application is an ASP.NET MVC3 site that utilizes JavaScript, jQuery and Ajax-JSON. This new web application is better adapted
for use on smaller screens, such as smartphone screens, than the current system. More about the proof-of-concept application in section 5 of this report.

To recapitulate, this report attempts to answer the following questions:

- What new risks, if any, would smartphone access to Strödata’s business system cause?
- Could the smartphone access decrease or even completely remove any existing risks posed to Strödata’s business system?
- Is it possible to implement access to Strödata’s business system from computers, smartphones and anything in between the two?
- What would be a satisfying way to implement access to Strödata’s business system for anything between computers and smartphones?
2 Background & Theory
The company Strödata, where this thesis project will be performed, has a web based business system (meaning a web application accessible through the internet). The system is used for most things related to the company, from planning work to reporting work or creating and modifying projects (which are collections of tasks, generally work orders but there is no set definition of what a project may or may not contain). See Figure 2.1 for examples of activities the system is used for. The system has been in use since 2004 with various updates applied since it was deployed. Since the business system is web based it can be accessed from anywhere as long as you have internet access and a computer. This mobility is one of the main reasons Strödata chose to use a web based solution for their business system.

To show how the employees at Strödata use the business system, some of the use cases for the system are shown in a simple use case diagram, as described by McLaughlin, Pollice and West [7], in Figure 2.1 below. Since the use case diagram is lacking in detail on how the system is used and in which situations it may be used, the use case diagram also does not show how the employees of Strödata wish it could be used. Therefore the use case diagram is followed by a use case scenario which incorporates a number of different use cases and shows how they might be used in a Strödata-employee’s typical day as well as some of the ways the employees wish it could be used.
Peter is employed by Strödata, he has just finished his current assignment and he wonders if he could fit in another client assignment before the day is over. Of course, he still needs to create a work report for the finished assignment and when that is done he needs to find a new assignment. To access the business system he would need a computer with internet access. He has the work laptop in the car and he does have his smartphone with internet access. Connection the smartphone to the laptop for internet access would do the trick. It would be a bit of a hassle though. He reasons that he might as well just drive to the office, connect his laptop to the wireless network, log in to the business system and create the work report there. After that there won’t be much left of the work day, Peter considers the idea of using some of his stored flex-time and go home early. But he doesn’t know how much flex-time he has stored. Both the creation of the work report and checking how much flex-time he has stored are simple enough tasks once you are logged on to the business system. It is too bad I can’t use the smartphone for this, Peter thinks. The elements of the web-application bleed into each other and cover each other making everything unreadable and unusable. It would have been easier and quicker if it had worked. He could have created the work report and checked his flex-time in the customer parking lot. Following that line of thought, Peter thinks of the
possibilities of smartphone access to the business system. If he could see the available assignments on his smartphone, he could pick one of them and the customer information could be used by the GPS-navigation application in his smartphone. That way he wouldn’t have to take notes on the distances he drove to and from customers either. Or the time he spent working on the assignments once he was there. It could all be collected by the smartphone. But what if I drop my smartphone? Peter thinks. Anyone who finds it can gain access to the business system and all the information in it. What if someone steals the smartphone to gain access to the information? We would really need to look into that if we ever consider enabling smartphone access to the business system.

As is mentioned in the use case scenario above, accessing the system from smaller, hand-held, devices is at the time of writing not an option since the web application is not adapted for smaller screens. The use case scenario also implies that accessing the system using a smartphone or another hand-held device is the next logical step for this type of system, the mobility of the business system would increase even further with smartphone access.

Most people these days (March, 2011) have a smartphone and at an IT-company such as Strödata, everyone has one. So, what is a smartphone and why could it be beneficial to have access to a company’s business system through one?

A smartphone is defined as [2]:

“A mobile phone that is able to perform many of the functions of a computer, typically having a relatively large screen and an operating system capable of running general-purpose applications.”

As the definition above shows, a smartphone is basically a personal computer in a smaller format. So, why/how could it be beneficial to enable access to a business system through such a device? There are not many people that do not carry a cell phone with them everywhere they go. Since the employees of Strödata have replaced their old cell phones with smartphones, they will have them at hand when they are at work, in the offices or on any of their customer’s premises. This would give them access to the business system whenever they need it. The same can of course be done using a laptop with internet access, but the employees may not always carry a computer with internet access with them, as opposed to their smartphone. A requirement from the employees is that they should be able to create a work report in a simple and quick manner, therefore the smartphone is a natural way to go. To be able to use smartphones to access the business system, the smartphones needs to have internet access. The internet access for the smartphones is provided by the telephone network operator. According to the telephone network operators there is good data-traffic coverage in the area where Strödata’s customers are located, which means that the employees should have internet access on their smartphones while working.

Two points to consider in Strödata’s case: There is already some level of smartphone access to the business enabled at Strödata. The employees are using their own smartphones to access company data. For example, the employees have access to their company e-mails through their smartphones. The employees also try to access the current business system through their smartphones. However since the business system is not adapted for smaller screens, the content of the web pages is largely unreadable. The functionality of the web application (aside from the readability problems on smaller devices) is sound. The functionality cannot be used on smartphones or tablets, since the elements of
the pages overlap each other to such an extent that they cannot be read/used. If one could distinguish which input-field corresponded to which label one could for example create a work report. The functionality is present and would create the necessary posts in the database for a complete work report. The application was created in 2004, at that time the available technology and techniques were not created with the intention of being used on smaller screens than regular computer screens. There were no such things as smartphones or tablets available at that time, the possibility was not something that was taken into consideration when implementing web applications at that time.

The fact that (employee owned) smartphones are present on the company network presents risks to the network and the systems that are connected to the network. Strödata embraces the Bring Your Own Device (BYOD) trend concerning smartphones, which is why employees are allowed to use their own smartphones to access company information. BYOD is explained in the literature [13] as:

“The Bring Your Own Device model/paradigm ... is now widely adopted to refer to mobile workers bringing their own mobile devices, with their data and applications, into their workspace for both working and personal use.”

If employees are allowed to bring and use their own devices in a company setting, there must be some policies on how these devices are (not) allowed to be used in order for the IT department to manage the devices. There should also be policies in place to help ensure the information security and reduce the risks posed to the system. [13]

There are of course different approaches to BYOD, and different levels so to speak. The “levels” depend on how the control and the responsibility is distributed between the employee and the employer. If the employer wishes to have control of the device, they have the option of buying it for the employee. Thereby owning the device which would give the employer more or less complete control of the device itself and which software it runs (which applications are allowed to access the business network and data). There is also the option where the employer provides a fixed amount of money that the employee can add to when selecting a device. This would give the employer a degree of control of the device and the software it contains while the employee has a more freedom regarding which device that is purchased. There is also the option where the employee purchases the device without the employer’s involvement. In this case, the employer has no control over the device (apart from what the employee agrees to) or the software on the device. The control and responsibility regarding the device is shifted towards the employee throughout the options to where the employee is fully in control and has full responsibility of what is caused by the device and the software it runs. [14]

There are both advantages and disadvantages of BYOD. Among the advantages there is the employee satisfaction. The satisfaction level of the employee increases when the employee is allowed to use a device of their own choice. The employees choose the device they prefer to use and work with leading to the employee being satisfied with both being able to choose as well as using a device they prefer. Another point to consider is that the employee can work with a device and software they are already familiar with, thereby reducing the cost for education in the system for the employer. This also increases the employee’s productivity. And of course, the employer spends less on the purchase of devices for employees if they are allowed to bring their own or if the employer only pays for part of the cost. [13, 14]
Something that can be either an advantage or a disadvantage depending on how the company decides to implement BYOD is the cost of device support. If the employer decides to provide the employees with devices they are allowed to use outside of work as long as they follow company policies, there is an increased cost of support for these devices. If the employees are completely responsible for the devices themselves, the cost of device support is lower. [14]

One of the disadvantages of BYOD mentioned in the literature [13] is the variety of devices the employees may bring to the business. If the employer has an application that every employee needs in their daily work, this application must be provided and maintained for multiple platforms. There are of course also security concerns. Some of which [14] are the increased risk of introducing malware to the company network through the use of employee owned devices that are used in other settings than in a work setting. The migration of sensitive company data from company owned devices to employee owned devices that are brought outside the company and used in the employee’s daily life. A lost or stolen device that contains sensitive company data may cause the business large problems. On an employee owned device which is also used for business purposes, there will be a mixture of company and personal data stored on the device. Should the company be allowed to track the device and thereby the employee since there is company data stored on the device?

Considering the advantages and disadvantages listed above, in what ways does it benefit Strödata to embrace the BYOD trend for employee smartphones, and in what ways is it a disadvantage for the company? Looking at the diversity of devices among the employees of Strödata it is clear that they have chosen a device they are comfortable with, and when speaking to the employees it is clear that they would find it difficult and more than a little annoying to be handed a device outside their comfort zone and being told they are only allowed to use that device for work. For example, if Strödata purchases HTC Android smartphones for all employees to use (only for work related tasks), the employees that prefer the iPhones or Windows-phones would be uncomfortable in this new environment. This applies to some extent to those who are used to a different version of Android as well. The same is true for any combination of devices, since most major operating systems (iOS, Android and Windows) are represented within the ranks of the Strödata employees. The fact that they probably already have dismissed these devices when they have purchased their own device, choosing one operating system over the others, would increase the discomfort. If Strödata would provide the employees with a specific smartphone to use during work it would also increase the cost of both device purchase as well as the cost of training in the use of the device for a part of the employees. This cost could present itself as either a cost of a training course or as an increase in time when performing tasks on the device. One advantage with company provided work-devices (in this case smartphones) is that they can be controlled by the company, there can for example be application white-lists containing which applications are allowed on the device and for use with company data. In a BYOD organization, the company has less control over the device. In Strödata’s case the policy is that if the employee wishes to have access to company data (at the time of writing, the employees company e-mail) they must allow remote wiping of the device. This policy is in place to help keep company data safe if the device is lost or stolen. A complete wipe of devices is also to be performed if a device that has had access to company data (this goes for all devices such as smartphone, tablets and laptops) before it leaves the possession of the employee. At the time of writing, there are neither any policies in place nor any capabilities to track the employees using their devices on behalf of the company. There are however thoughts of how this could be used to measure driving distance to and from customers. This idea was presented during this project thesis by multiple employees as a way to decrease the workload
in regards to creating work reports, where the distance travelled to perform a task for a customer is required. At the time of writing Strödata does not have any specific applications for smartphones that the employees need access to, however since smartphone access to Strödata’s business system is part of this project thesis it is worth mentioning. Since the employees at Strödata have different operating systems on their smartphones, Strödata must maintain several versions of any application which gives access to the business system. If it is decided that access to the business system shall be possible through a smartphone application. This will of course cost the company enough money to be noticeable. Another cost is that the applications must be tested, to verify that they are still functional, each time any of the operating systems are updated. If they are not fully functional after the update, the applications must be updated as well. Each time a new operating system is introduced to the business a new version of the applications must be implemented.

If a business is considering to allow smartphone (BYOD or otherwise) access to their business system it is, to say the least, wise to consider the risks and disadvantages and not only the benefits. In 2010 the European Network and Information Security Agency (ENISA) released a report regarding smartphones and what risks and opportunities they may present. In the report, the general risks [9] are divided into usage scenario categories, where the type of user is considered when regarding the risks, more on this division below. The risks [9] that are discussed are described in Table 3 below.
<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data leakage</td>
<td>Unprotected data on a smartphone can be accessed by an attacker once the attacker has access to the smartphone.</td>
</tr>
<tr>
<td>Improper decommissioning</td>
<td>When decommissioning a smartphone all sensitive data must be purged from the smartphones’ memory.</td>
</tr>
<tr>
<td>Unintentional data disclosure</td>
<td>Users are either not aware of, or do not use, privacy settings in smartphone applications (when they are available) to prevent the application from transmitting data to unknown destinations.</td>
</tr>
<tr>
<td>Phishing</td>
<td>User information (account names, passwords etc.) is collected by applications that present themselves as something else or through emails or SMS-messages.</td>
</tr>
<tr>
<td>Spyware</td>
<td>Spyware that is installed on a smartphone can give an attacker access to personal information.</td>
</tr>
<tr>
<td>Network spoofing attacks</td>
<td>Through the use of a rouge access point which the smartphone connects to, an attacker can act as a man-in-the-middle, which can lead to further attacks.</td>
</tr>
<tr>
<td>Surveillance</td>
<td>A smartphone is targeted to be used to spy on an individual user.</td>
</tr>
<tr>
<td>Diallerware</td>
<td>Diallerware that is installed on a smartphone can for example make hidden in-application purchases or uses payment SMS-messages or starts calls to payment-numbers.</td>
</tr>
<tr>
<td>Financial malware</td>
<td>Financial malware specifically targets a users’ financial information, for example credit card numbers or bank account numbers.</td>
</tr>
<tr>
<td>Network congestion</td>
<td>All network resources are used resulting in a denial-of-service situation for the user.</td>
</tr>
</tbody>
</table>

Table 3 Risks [9] discussed in Smartphone security: Information security risks, opportunities and recommendations for users.

The risks that are presented above are general risks in connection with smartphones. As smartphones and these risks already are a part of Strödata’s daily life and not specific for smartphone access to the business system some of these risk will be either regarded as outside of the scope of the risk analysis that is a part of this project thesis or as part of general risks posed to the system.

As mentioned above regarding the risks [9] that are presented, there are different usage scenarios described, each usage scenario represent different levels of users. Table 4 describes the usage scenarios [9]:

---

9
### Usage scenario

<table>
<thead>
<tr>
<th><strong>Usage scenario</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consumer (C)</strong></td>
<td>The smartphone is an integral part of the consumer’s daily life – and is used for everything from phone-calls to banking errands.</td>
</tr>
<tr>
<td><strong>Employee (E)</strong></td>
<td>The smartphone is used by an employee in a business or government organization. It is used for business related activities, such as business phone-calls, e-mail conversations and video conferences. The employee may use business specific applications on the smartphone. The smartphone may be used for personal use as well, as described in the consumer usage scenario. The employee’s use of the smartphone in a business setting is regulated by IT policies. These policies are set by the employer’s IT officer.</td>
</tr>
<tr>
<td><strong>High official (H)</strong></td>
<td>The smartphone is used by a high level official in a business or government organisation (or by that person’s assistant). The smartphone is used in the same manner as in the employee usage scenario, with the addition of it being used to handle sensitive data and tasks. The employee’s use of the smartphone in a business setting is regulated by IT policies. Additional policies are in place compared to the employee usage scenario. For example, the smartphone may be configured to encrypt all data it contains. These policies are set by the employer’s IT officer.</td>
</tr>
</tbody>
</table>

**Table 4 Description of usage scenario levels [9].**

The usage scenario division [9] is quite useful when performing when performing an analysis of a risk and how it would affect different user-groups that have access to different amounts of information. As well as performing different tasks on the system that is to be analysed. For example, the information an employee has access to is probably not as extensive as the information a high official within the same company has access to. Or it could be the reverse, the high official does not have access to the level of detail that an employee may have. It is important to keep track of which users/user groups have and should have access to what information, both when setting up a system and when analysing a system. In the case of smartphones one must expect different users to make use of their smartphones in different way depending on their work assignments and positions within a company. It is also stated [9]:

“It should be noted that individual smartphones and smartphone users frequently cross-over from one usage scenario to another.”

One should keep in mind that users may change their behaviour during different situations. This includes their behaviour regarding their smartphone use. Which in turn affect how the risks are viewed and the consequences they may result in.

In regard to the above mentioned risks, there are several precautions that can be taken. Some of these are common for any system, for example requiring passwords and/or PINs to access systems or information, or keeping software up-to-date. There are of course many lists of precautions to take to secure your data and IT-systems, both specifically regarding smartphones and in general. The list that is presented below is a compilation of three different lists [12]. One list for each of the smartphone operating systems: Android, BlackBerry and iOS. The list-items from the three different lists have been
categorized in the compiled list that is presented below. This was done because the three different lists do not have identical list-items but they do have very similar items in each of the categories.

Awareness

- Basic web security awareness. The users are required to have basic web security awareness, for example: The user is aware that conducting sensitive transactions on public networks is to be avoided. Such transactions should be performed on trusted networks.
- Root. If a device is rooted/jailbroken, that means the user has administrator privileges on the device. However, the same is true for an attacker who has managed to infiltrate the device.
- Malware spreading and interception of messages. The user should be aware that e-mails and SMS messages can be intercepted and that malware can be spread using these services.
- Location of the device. The user should be aware of the location of the device. Most spyware require physical access to the device to be installed.

Data Storage

- Make frequent back-ups for the data stored on the device to prevent loss of data.
- Minimize the amount of personal data that is stored on cloud services. The data may not be entirely secure where it is stored in the cloud.

Applications

- Avoid applications from unofficial sources. These applications are at high risk of containing malware.
- Make sure to review the permissions the application requires. Many applications require more permissions that what should be needed to perform their functions. For example, a single player game that requires access to the location of the device.

Security Settings

- Enable auto-lock. Locking the device automatically after a short period of time. This lowers the chance that someone can access the content of the device.
- Enable a password protection. Requiring a password to unlock the device is a good first line of defence. Also, using different passwords for different devices, applications and services is recommended.
- Minimize the amount of information that is displayed on the lock-screen of the device. This reduces the amount of information that can be gleaned from a locked device.
- Install anti-virus software. Anti-virus software is good at detecting previously identified malware. However the requirement that the malware has been identified and a signature has been established makes it less effective to new malware and custom created malware.
- Install and configure a firewall. The firewall will prevent any unauthorized connection to or from the device. This can include SMS and MSS as well.
- Keep the system up-to-date. In new versions of software, security flaws are often fixed.
- Enable remote wiping of the device. If the device is stolen or lost, the ability to remotely wipe the data on the device will keep any sensitive information out of the wrong hands.
The ENISA report [9] also includes a section of recommendations on how to deal with some of the risks that have been brought up previously in the report. They choose to only include recommendations regarding the risks with the highest priority, as they explain in the beginning of the report section:

“In this section we make practical recommendations for smart smartphone end-users, IT officers and CISOs dealing with smartphones. We take a pragmatic risk-based approach, prioritising the high risks.” [9]

In this section of the report [9], they emphasise that that users often switch between the different usage scenarios that have been described in the report and above by writing:

“We reiterate that smartphone users frequently cross over from one usage scenario to another. In order to mitigate any potential risks this introduces, IT officers should anticipate and even assume that this will occur and issue policy and guidance on safe use.” [9]

The list of recommendations will not be presented here as it contains recommendations for each usage scenario for each of the risks (using the designations the risks have been given in the report [9]: R1-R9. Presenting them here would take up quite a lot of space and all the recommendations can easily be found in the report [9] section 4, pages 43-48. To give a sense of the nature of the recommendations, perhaps it is enough to say that they are as detailed as the risks the report contains, and that have been presented above and that the recommendations section is worth reading for the interested reader of this project thesis.

The Federal Communications Commission (FCC) has also issued a checklist of precautions to take in regard to smartphones [10]. The list from the FCC contains ten precautions regarding smartphone security, described below:

1. To prevent unauthorized access to your smartphone, set a password or Personal Identification Number (PIN) on your phone’s home screen as a first line of defence in case your phone is lost or stolen. You should also configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones.

2. Do not alter security settings for convenience. Tampering with your phone’s factory settings, jailbreaking, or rooting your phone undermines the built-in security features and makes the smartphone easier to an attack.

3. You should backup data that is stored on your smartphone. This allows for simple restoration of the data to a new smartphone if the current smartphone is lost, stolen, or erased.

4. Before downloading an app, make sure it is legitimate. For example by: checking reviews, confirming the legitimacy of the app store, and comparing the app sponsor’s official website with the app store link. Many apps from untrusted sources contain malware that can steal information, install viruses and/or damage your data.

5. Make sure to check and understand the privacy settings for every application that you install on your smartphone.
6. An important security feature for smartphones is the ability to remotely locate and wipe your phone.

7. You should keep your phone’s operating system software up-to-date by enabling automatic updates or accepting updates when prompted. Keeping your operating system and applications up-to-date you reduce the chance that you fall victim to an attack focused on known and fixed vulnerabilities.

8. Limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless. Also be wary of clicking links and entering sensitive information.

9. Since your smartphone very well may contain sensitive data, make sure to wipe it before disposing of it.

10. If your phone is stolen, report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider.

Most of the precautions that are contained in the three lists, two of which are presented above, can be divided into categories. The categories I have identified are:

- Passwords and PINs to access the device as well as data.
- Updates to the smartphone software should be installed.
- Security applications should be installed on the smartphone.
- Understanding and caution on behalf of the users is very important.
- Encryption of the smartphones memory should be enabled.
- Disposal of smartphones, the procedure of the disposal.
- Remote wiping of the smartphone should be enabled.

At Strödata, most of these categories are handled. Passwords and PINs are mandatory for the employees’ smartphones, so is encryption and remote wiping. Installing updates for the employees’ smartphones is an obvious element of smartphone use for the employees at Strödata. Security applications on the employees’ smartphones is not mandatory, however none of the employees I spoke to in regard to smartphone risks lacked security software on their smartphone. Both understanding and caution regarding applications and use of smartphones is well spread in the company. Each employee has a proper understanding of these precautions. There is also a procedure in place for smartphone disposal containing memory wiping and a complete reset of the smartphone to the factory settings.

Accessing the system through a smartphone may cause new risks to the system. To see how smartphone access affects the risks posed to the system, a risk analysis needs to be performed on the system. First on the system in its current state, and second to determine how the smartphone access will affect the risks posed to the system. In the analysis of the current system, the risks that are found need to be managed. Risk analysis is described by Luker and Petersen [3] as:

“Conducting a risk analysis is a process of identifying assets, the risks to those assets, and procedures to mitigate the risks to the assets.”

Risk analysis is defined in a similar way by the National Infrastructure Protection Center [4]:

13
Simply stated, risk management is a systematic and analytical process by which an organization identifies, reduces, and controls its potential risks and losses.”

Basically, the activities that will be performed are:

- Asset assessment
- Threat assessment
- Vulnerability assessment
- Risk assessment

This means that the Strödata’s assets will be assessed (identified and consequences calculated, should anything happen to each asset). Threats to the system will be identified as well as vulnerabilities in the system. The risks that the threats combined with the vulnerabilities pose to the assets will be assessed as well (the likelihood that they occur combined with the consequences they will have should they occur). Treatments for the risks will also be identified in order to reduce the likelihoods and/or consequences of the risks. Could accessing the system through a smartphone be a treatment? If it can, how will it affect the risks? Will such access introduce new risks? What new risks, and what could their consequences be? As mentioned previously, a new risk analysis needs to be performed to see how the smartphone access would affect the system.

Hazard & Operability Studies, Fault Tree Analysis, Event Tree Analysis, Failure Modes and Effects Analysis, What-if/Checklists and CORAS are some of the risk analysis methods that are available. The National Infrastructure Protection Center describes a method of risk analysis and management [4], which is rather general. As such it can be used for any type of system. However, that is also a downside of it. The method may be too general to be the best method for any given situation. All the methods listed above contain the same general activities that are listed above.

These steps are often accompanied by identification of possible countermeasures that will reduce the risks (reducing the threats and/or consequences). The differences between the above mentioned methods are how they perform the analysis and what type of system they are adapted for.

Below, the different risk analysis methods that are listed above are described.

**Hazard and Operability Studies**

The Hazard and Operability Studies analysis method consists of a table containing Guide words, Deviations, Possible causes, Consequences and Required actions. The guide words depend on the system that is to be analyzed, and should have an effect on the system. Hazard and Operability Studies gives a more structured way of performing What-if analyzes, based on the guide words. The guide words are the base of the what-if argument and have a direct connection to the Deviations in the system. The deviations have possible causes and consequences, the required actions are actions that are required to prevent or mitigate the consequences [8, 11].

The Hazard and Operability Studies method is suitable to identify deviations from the normal flow in a system and to find problems in the current flow and is used mainly for systems where the flow is important. The method requires several viewpoints of the system and the team of analysts need knowledge of all the parts of the system [8, 11].
**Fault Tree Analysis**

The Fault Tree Analysis method consists of fault trees. The root of the tree is a specific undesired fault event. The branches leading to the event represent scenarios. Each scenario can be a basic event, a fault event, an undeveloped event or a human fault. The branches of the tree are joined by and/or gates. To reach a fault event, one (or-gate) or more (and-gate) events are required to have happened before. In short, you start with the undesired event and work backwards through the events that may lead to the undesired event [8, 11].

Fault Tree Analysis is good for analysing specific undesired events but it requires a skilled analyst and a well defined and accurate model of the system [8, 11].

**Event Tree Analysis**

The Event Tree Analysis method consists of event trees. Each event tree starts with a single event at the root and branches out from there. Each new split in the trunk represents a new event, where the new branches represent the possible outcomes from the event. At the end of each branch the frequency of the outcome as well as the consequence is presented [8, 11].

Event Tree Analysis is well suited for systems with multiple safeguards in place but requires a well defined and accurate model of the system [8, 11].

**Failure Mode and Effects Analysis**

The Failure Mode and Effects Analysis method consists of a chain of events, starting with a single event that is caused by a failure mode, which leads to undesired outcomes. Failure Mode and Effects Analysis is focused around components, one error/failure of a component is caused by one or more failure modes which leads to undesired effects. The analysis also includes possible methods to detect and/or mitigate the undesired effects as well as recommendations to prevent the failure mode from occurring [8, 11].

The Failure Mode and Effects Analysis method is suitable for modelling failures caused by a single event but requires that the analyst has a good understanding of the systems failure modes and a well defined and accurate model of the system [8, 11].

**What-If/Checklists**

The What-If/Checklists risk analysis method consists of two parts, a What-if analysis and a Checklist analysis part. The What-if part of the analysis method is a rather unconstrained analysis method, where the participants brainstorm to create different “What if...”-scenarios which are then applied to the target system. The checklist analysis part involves checking of different scenarios from predefined checklists [8].

The What-if/Checklists analysis method does not require a large amount of training on behalf of the analysis team [8]. However, it is also rather unstructured.
The CORAS analysis method consists of seven steps. First is the introduction to the target system. Second is a high level analysis of the target system. Third is the approval step. Fourth is risk identification. Fifth is the risk estimation step. Sixth is the risk evaluation. Seventh, and last, is the risk treatment step. Each of the steps has predefined outputs in the forms of diagrams and tables [1].

The CORAS analysis method is well suited for IT-systems, it is also well structured and suitable for an inexperienced analyst [1].
3 Risk analysis

The question that this section of the report will answer is “what is a risk analysis?” A risk analysis is an analysis of a system that identifies risks posed to the system in order to better protect it. As well as protecting it in a suitable way, the defences and their cost should be in proportion to the damage the system would take if the defences are not in place. There are many different methods to perform a risk analysis (some of which are mentioned below) and they are adapted for different situations (different systems and different organizations). The choice of risk analysis method is briefly discussed below.

To perform the best possible risk analysis for any system, a suitable method must be chosen.

Some of the available risk analysis methods are Hazard & Operability Studies, Fault Tree Analysis, Event Tree Analysis, Failure Modes and Effects Analysis, What-if/Checklists and CORAS. The National Infrastructure Protection Center describes a method of risk analysis and management in its report [4], which, as mentioned in section 2 of this report, is rather general.

All the risk analysis methods that are described in section 2 have their uses and their strong points. All are not suited for the same type of system or the same type of analyst. Their compatibility with different situations are also varied. For example, the What-If/Checklist analysis method may not be the best suited for a very in-depth analysis of a complex system, performed by a very inexperienced analyst. But the What-If/Checklist method may be the perfect method for a semi-experienced analyst who is to perform a high-level analysis of a smaller system. For this project thesis, this target system and this analyst, it is probably not the perfect match since it is not very structured or generates sufficient output to create a thorough report. The same arguments can be used in the case of the general risk analysis method described by The National Infrastructure Protection Center [4]. The Hazard and Operability Studies analysis method is focused on the flows in the system. In this project the focus is not on the flows of the system but rather access to data and to physical devices. The focus on flows makes the Hazard and Operability Studies analysis method less of an option and the method is better suited for nuclear processes than IT-systems [8]. The Event Tree Analysis method and the Fault Tree Analysis method could both be suited for the type of system that is the target in this project thesis. They both generate output that will be presentable in a report, however the output diagrams will not be as clear as one might wish. The tree-structure may become quite confusing when faced with the output of a complex system. The sheer amount of tree-diagrams could be overwhelming to the reader. When considering the output that is generated by the Failure Mode and Effects Analysis method, which would be a rather large table. A table of that size could also be confusing and make it difficult for the reader. For this reason, none of the three methods is suited for this thesis project. The output from CORAS analysis method consists of both diagrams and tables, making it better suited for a large report. The output differs in the different steps of the analysis and can be presented in a structured manner, as opposed to one large table for example. The diagrams can, when structured well, be very clear unless there is too much information in them. None of the tables are expected to be overly large and can be presented easily in a report. The structured approach of CORAS is also appealing to an inexperienced risk analyst without an experienced team to work with. The fact that CORAS also focuses on cooperation between departments/disciplines of the target system is also appealing. Input from people in different roles, that use the system in different ways will give a more complete view of the system that a single analyst could provide.
The CORAS analysis method described in *Model-based security analysis in seven steps – a guided tour to the CORAS method* by den Braber et al [1] will be used for the risk analysis part of this project thesis, due to the reasons and arguments mentioned above. Below follows further information about the CORAS analysis method, further information will follow in the subsequent sections.

CORAS is also a well structured method for risk analysis, which suites an inexperienced risk analyst like myself well. According to den Braber et al [1], CORAS has seven steps which are listed here:

1. Introduction
2. High level analysis
3. Approval
4. Risk identification
5. Risk estimation
6. Risk evaluation
7. Risk treatment

These steps will be explained further in the following part of the report. Each of the steps will have a separate section and each section will contain an explanation of what the corresponding step entails, such as activities to be performed as well as the required output (diagrams, tables etc.) from these activities, including explanations for each output.

For the CORAS analysis to be as complete as possible, the analysis must incorporate as many viewpoints of the system as possible. Receiving input from as many places and as many different roles as possible. The more viewpoints that are incorporated into the analysis the more of the system and the possible threats, scenarios and so on can be identified and analyzed. To incorporate as many roles and viewpoints as possible, meetings and/or discussions will be held in each of the steps that CORAS consists of. For some of the meetings and discussions the analyst may have prepared a crude initial view of for example the threats posed to the system. This initial view will then be refined during the meeting and the following discussions will increase the detail and completeness of the analysis. In each of the steps, which are presented in the sections below, an explanation of how the meetings and/or discussions were conducted will be presented.

In CORAS, everything is modelled in a specific manner. UML-diagrams are used to describe the system. Other diagrams in the risk analysis (asset-, threat-, risk- and treatment-diagrams) as well as tables (high-level threat table, likelihood table, consequence tables etc.) are described in a CORAS specific manner. These CORAS-specific diagrams and some of the tables contain certain CORAS specific icons. In Table 5 below, the CORAS-icons what they represent is presented.
3.1 Introduction

In this step of the analysis the objective is to be introduced to the system that is going to be the target of the analysis. A good understanding of the system is required to perform a good risk analysis, knowing what to protect is key. Figure 3.11 shows my understanding of the system after an initial meeting with representatives from Strödata where I was introduced to the system. The initial meeting was between myself, the analyst, and the CTO. During the meeting the representative from Strödata explained how the system works and how its’ different parts are connected without going into very much details. Figure 3.11 is a rendering of the sketch that was drawn during the explanation of the system. During the meeting the target of the risk analysis was also discussed. Should it be the system in its entirety, including the SSL-connection, the browsers the employees use and so on, or a subset of all the things that could be included in the system? The discussion leads us to the size of the project thesis and how much could be included and how much that actually should be included. Performing a risk analysis on a system that includes such things as the entire internet, all possible web browsers the employees may use would be a large task. Such a large task would not be suited for this type of project theses. It was decided that we should narrow the scope to what would be most useful to the task. The point of the risk analysis of the business system is to create a baseline for the further analysis of how smartphone access would affect the risks posed to the business system. The target definition is presented below. The goal of the risk analysis was also discussed during the meeting, and is presented below.

Figure 3.11 System overview

The Strödata employee uses an internet browser on his/her computer to access Strödata’s web-based business system. The connection between the employees’ computer and the web application
(Strödata’s business systems web application will be referred to as “WebApp” from here on) uses SSL for protection. The traffic goes through at least one firewall (located on the server-side). The WebApp communicates with the database on the server to get the information the employee requests, and inserts the information the employee provides into the database.

The target of the analysis is Strödata’s web based business system itself, meaning the web-application, the database and the physical server. Examples of what is out-of-scope are communication between server and client, network capacity, network redundancy, the firewall. It is also decided that the operating system on the server is out-of-scope due to the need to limit the scope in combination with Strödata feeling that they already have a working structure regarding the operating system in place.

The goals of the analysis are to increase the understanding of the current business system, as well as the risks the system is subjected to at the present, and to create a baseline for a comparison and an evaluation of how smartphone access to the system would affect those risks.

### 3.2 High-level analysis

In the second step of the analysis we go deeper into the system, describing it in a series of diagrams. These diagrams are created by myself, the analyst, and then presented to representatives of the client, Strödata, during a meeting. Present at the meeting (in addition to myself, the analyst) was the CEO and the CTO. The meeting participants representing Strödata either accept the diagrams as accurate descriptions of the system, or not. In the case that a diagram is not accepted as accurate, the client points out where changes are needed. The changes are made before presenting the result to the client again for inspection. The inspection-acceptance-correction loop is repeated until all the diagrams are accepted as accurate. In addition to the presentation of the system description, the assets of the system are discussed, identified and described in a table and a diagram during the meeting. A rough risk identification is also performed, resulting in an initial high-level threat table containing a combination of threat scenarios, unwanted incidents and assets, threats and vulnerabilities. After the meeting, the scenarios in the table are then modelled in CORAS-specific diagrams, creating initial threat diagrams.

The following section deals with the high-level analysis of Strödata’s web-based business system based on my understanding of it at the time of writing.

Figure 3.12 shows the structure of the business system divided into classes, each class represents a different part of the system. An employee uses an employee PC, which may send information through a firewall. The information then travels across the internet towards the server where the business systems web application is running. The information reaches the web application through a firewall. The web application then communicates with the database to retrieve or deliver data. Entities to note are the “SSL-connection”-class, which shows that the connection between the employees PC and the WebApp is a SSL-connection. There is also the “Focus” area which shows which parts of the system the analysis will focus on (the target).
Figure 3.12 Class diagram showing a conceptual view of the target

Figure 3.13 is a collaboration diagram that shows the communication-lines between the employee PC and the server with the WebApp and the database. Notice that the left firewall is within parenthesis, the reason for this is that there is no guarantee that there is a firewall in front of the employee PC when they are on assignment. The employee may be using a computer without a firewall in place between it and the internet.

Figure 3.13 Collaboration diagram illustrating physical communication lines

Figure 3.14 shows the sequence of events for when an employee performs the task of work reporting in the business system.
Figure 3.14 Sequence diagram for the “Reporting work” task

Table 6 and Figure 3.15 show the assets of the stakeholder Strödata. In Table 6 the assets are named and described. The diagram in Figure 3.15 shows how the assets affect each other. The arrows in the diagram illustrate which assets affect others. For example the “Physical server”-asset affects all the other assets. If that asset is harmed in some way, the assets it affects will also be harmed. This relation between assets will be used when creating threat diagrams later in the analysis. The coloured assets within the border are direct assets (see Figure 3.1) while the “greyed” assets outside are indirect assets (see Figure 3.2) to the stakeholder (see Figure 3.5) Strödata.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer database</td>
<td>The database where customer information is stored.</td>
</tr>
<tr>
<td>WebApp</td>
<td>The web application that is used to communicate with the database.</td>
</tr>
<tr>
<td>Physical server</td>
<td>The physical server where the WebApp and the “Customer database” are located.</td>
</tr>
<tr>
<td>Customer trust</td>
<td>The trust the customers have in Strödata and in Strödata’s system.</td>
</tr>
<tr>
<td>Customers system</td>
<td>The customers’ systems which Strödata set up and/or maintains.</td>
</tr>
</tbody>
</table>

Table 6 Initial asset descriptions
Table 7 is an initial high-level threat table and it contains information about different scenarios that may occur. Each scenario consists of a cause (a threat that can be intentional or not, human or not, see Figure 3.7 - Figure 3.9), a scenario which describes what happens and what is affected using risks (see Figure 3.3), unwanted incidents (see Figure 3.4) and assets. Finally the scenarios contain vulnerabilities that make the scenario possible (see Figure 3.6).
<table>
<thead>
<tr>
<th>Who/What is the cause?</th>
<th>How? What is the incident? What does it harm?</th>
<th>What makes it possible?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>Breaks into the system and changes customer information in the database.</td>
<td>Insufficient security</td>
</tr>
<tr>
<td>Hacker</td>
<td>Breaks into the system and steals customer information from the database.</td>
<td>Insufficient security</td>
</tr>
<tr>
<td>Hacker</td>
<td>Customer information leaks out, no longer confidential. Harms the trust in Strödata and the system.</td>
<td>Insufficient security</td>
</tr>
<tr>
<td>Employee</td>
<td>Customer information leaks out, no longer confidential. Harms the trust in Strödata and the system.</td>
<td>Insufficient training</td>
</tr>
<tr>
<td>Employee</td>
<td>Sloppiness compromises integrity of customer information in the database. May harm the customers system.</td>
<td>Insufficient training</td>
</tr>
<tr>
<td>Employee</td>
<td>Forgotten details, causing erroneous information to be inserted into the database, compromising the integrity of customer information in the database.</td>
<td>Insufficient availability of the business system</td>
</tr>
<tr>
<td>System failure</td>
<td>System goes down.</td>
<td>Unstable technology</td>
</tr>
<tr>
<td>Network failure</td>
<td>Transmission problems compromise the availability of the web application.</td>
<td>Unstable connection /immature technology</td>
</tr>
</tbody>
</table>

Table 7 Initial high-level threat table

Each of the scenarios in Table 7 are transferred to initial threat diagrams, one for each type of threat (intentional human, unintentional human and non-human). As the risk analysis progresses the diagrams will change through input from Strödata. The diagrams have been used in later steps of the analysis to estimate the risk for each scenario. And later on the diagrams have been used as the base for treatment diagrams among other things.
Figure 3.16 shows the initial threat diagram for intentional threats. Intentional threats are threats that intentionally causes harm to the system. The diagram is divided into two parts, outside of the company and the inside the company (all CORAS-specific diagrams are divided in this manner). On the outside is the hacker threat and on the inside there is the employee threat, the vulnerabilities, the threat scenarios, the unwanted incident that follows and the assets that are affected. To better understand the diagram let us look at one of the scenarios represented in Figure 3.16. A “Hacker” is a threat to the business system. By exploiting the vulnerability “Insufficient security” the hacker can break into the system, that attack is the threat scenario. The attack leads to the unwanted incidents where both the confidentiality and the integrity of the customer database. The first unwanted incident affects both the”Customer trust” and the “Customer database” assets. The second unwanted incident affects both the “Customer database” and the “Customer system” assets. Since the integrity of the database is compromised an employee cannot trust information from the database about a customer’s system which may result harm to the system.

![Initial threat diagram for intentional human threats](image-url)

Figure 3.16 Initial threat diagram for intentional human threats

Figure 3.17 shows the initial threat diagram for unintentional human threats. An unintentional threat is a threat that does not intend to harm the system but that may do so by accident or due to carelessness etc. Figure 3.17 only has the “inside” part of the diagram since unintentional threats can only come from inside the company, in this case employees.
Figure 3.17 Initial threat diagram for unintentional human threats

Figure 3.18 shows the initial threat diagram for non-human threats. Non-human threats are threats that cannot be controlled, they could be power failures or earthquakes etc. In this case the threats are “Network failure” and “System failure”. The “Network failure” is not seen as a part of Strödata, since the failure may occur anywhere between the employees PC and the server, and is therefore “outside” while the “System failure” is on the inside for obvious reasons.

Figure 3.18 Initial threat diagram for non-human threats

3.3 Approval

In the approval step of the risk analysis the system-describing diagrams are shown to the client once again, in this case the diagrams were show to the CEO for final approval during a meeting. The client then either accepts them as accurate descriptions of the system, or not. Should the descriptions not be accepted as accurate, the client points out where changes are needed. As a result of this, a list of changes to make to the diagrams to make the description accurate is created and agreed upon. This step also includes the creation of a common likelihood scale, consequence scales for each of the assets, risk evaluation matrixes for each of the assets as well as a ranking of the assets in order of importance.
During the meeting with the CEO this issue was also raised. The scales and the risk evaluation matrixes were created in cooperation with the CEO.

To create the likelihood and consequence scales I, the analyst, created initial scales in order to have a starting point for discussions with the CEO, and later the CTO. The steps on the scales were to be kept but the values of each step were not. The process of creating the scales was a process of defining the values, or value ranges, for each step on the scales. Regarding the likelihood scale, one scale can be used. The likelihood value of an incident is not affected by the differences in the nature of the assets. It is merely a probability value of how often something happens in a given time span. The likelihood scale was, in comparison, easy to establish. For each of the steps in the scale I, the analyst, asked the question: How many times in a ten year period does a “rare” even occur. The result is presented below in Table 10.

The defining of the consequence scales was more difficult. Considering the different types of assets, the values of the same consequence varies from asset to asset. For the information-assets it was decided to divide each consequence step into three parts, one for each of the assets confidentiality, integrity and availability properties. After explaining that the values in the scale are not set in stone and that they do not need to be exact values. Value ranges with diffuse limits are perfectly fine. That the limits can be moved should they need to be, and if an incident should find itself on top of or close to the limit, the incident can be placed on either step of the scale, at the discretion of the client. And that the goal is to define values to the steps on the scale nothing more. For each step of the scale, for each asset, and where it was applicable for each property of the asset, I asked the question: What would a “catastrophic” incident cost regarding this asset? After giving all steps for all assets a monetary value, each value was reviewed again and adjustments were made where they were needed. The result was value-ranges in SEK for each asset, step and property.

Later in the risk analysis these estimated values are used, but should be noted that they are estimates and not precise actual values. Because of this the values that are found based on these estimates may be offset from the actual values. The estimates are however enough to create a reasonable picture of the situation the business would be in, should an asset suffer a (for example) catastrophic consequence. Both the scales and matrixes were also provided for the CTO so that he may provide his view of them. The feedback was then presented to the CEO and an agreement was reached for a final version of the scales and the matrixes, these are presented below. The ranking of the assets followed the same pattern. A ranking among the assets was created in cooperation with the CEO during the meeting, after the final version was decided (this is further explained below). This ranking was presented to the CTO, who agreed that this ranking was correct in his mind as well.

In the approval stage, the class diagram showing a conceptual view of the target (Figure 3.12), the collaboration diagram illustrating physical communication lines (Figure 3.13) and the sequence diagram showing the sequence of events for reporting work (Figure 3.14) were accepted as accurate. The initial assets (Table 6 and Figure 3.15) were not. The asset “Customers system” is not applicable, the system is not used in a manner such that it would cause harm to a customers’ system if the confidentiality, integrity or availability of the information is compromised. The “Customer database”-asset is divided into the discrete assets: “Company information”, “Customer information” and “Financial information”. The corrected assets are described in Table 8 below and the corrected asset diagram is shown in Figure 3.19 below.
<table>
<thead>
<tr>
<th>Asset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer information</td>
<td>The information about customers that is stored in the database. For example contact information which a competitor would find useful.</td>
</tr>
<tr>
<td>Financial information</td>
<td>The financial information concerning Strödata that is stored in the database. For example employee salary records and customer billing information.</td>
</tr>
<tr>
<td>Company information</td>
<td>The information about Strödata and its employees that is stored in the database. For example employee names and social security numbers.</td>
</tr>
<tr>
<td>WebApp</td>
<td>The web application that is used to communicate with the database.</td>
</tr>
<tr>
<td>Physical server</td>
<td>The physical server where the WebApp and the Customer database are located.</td>
</tr>
<tr>
<td>Customer trust</td>
<td>The trust the customers have in Strödata and in Strödata’s system.</td>
</tr>
</tbody>
</table>

Table 8 Asset descriptions

Figure 3.19 Asset diagram

The result of the asset-ranking is shown in Table 9 in order of importance (one being the highest and five being the lowest).

<table>
<thead>
<tr>
<th>Asset</th>
<th>Importance</th>
<th>Type</th>
</tr>
</thead>
</table>

28
Notice that the “Customer trust”-asset has the importance listed as “Scoped out”, this means that the asset will not be regarded in the analysis. The reasoning behind excluding this asset from the analysis is mainly due to the difficulty in measuring it. Also notice that the asset “Customer system” has the importance listed as “Not applicable”, as stated earlier this asset is not applicable since the system is not used in a manner in which it affects a customers’ system. The information in the database would not harm the customers’ system if the confidentiality, integrity or availability of the information is compromised. The other assets are ranked according to their importance to Strödata.

Table 10 shows the likelihood scale which was agreed upon. The information in the description column is presented in the following way: “number of times per ten years” : “10 years” = “number of times per year” : “1 year”. The likelihood scale will be used together with the consequence scales, which are also created in this step of the risk analysis and are presented further below, for each asset to determine if the risk is acceptable or if the situation requires further evaluation. The results of this will be displayed in risk evaluation matrices for the assets.

<table>
<thead>
<tr>
<th>Likelihood value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td>50+ : 10 years = 5+ : 1 year</td>
</tr>
<tr>
<td>Likely</td>
<td>21 - 49 : 10 years = 2.1 - 4.9 : 1 year</td>
</tr>
<tr>
<td>Possible</td>
<td>6 - 20 : 10 years = 0.6 - 2 : 1 years</td>
</tr>
<tr>
<td>Unlikely</td>
<td>2 - 5 : 10 years = 0.2 - 0.5 : 1 year</td>
</tr>
<tr>
<td>Rare</td>
<td>0 - 1 : 10 years = 0 - 0.1 : 1 year</td>
</tr>
</tbody>
</table>

The consequence scales below define the values of the consequence terms “catastrophic”, “major”, “moderate”, “minor” and “insignificant” in money (SEK) for each asset, mapping the terms to a corresponding cost. For the information assets, each consequence is divided into confidentiality, integrity and availability. This is done because the consequences differ between the different types of compromise for the information. For example, a catastrophic consequence for the asset “Customer information” regarding availability could mean that all customer information that is stored in the database is gone and all of the backups are unavailable, for whatever reason. This situation would cost Strödata 25 000 SEK or more. The cost has been calculated from the financial loss of the data as well as the cost to restore the data. The consequence scales will be used together with the likelihood scale in Table 10 to determine if a risk is acceptable or if the situation needs to be evaluated further. The results of this evaluation will be shown by the risk evaluation matrices. All of the information in the following tables and matrices has been defined through collaboration with the Strödata employees.

Table 11 shows the consequence scale for the “Customer information”-asset.
<table>
<thead>
<tr>
<th>Consequence value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Integrity</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>1 000 000+ SEK</td>
</tr>
<tr>
<td>Major</td>
<td>200 000 – 1 000 000 SEK</td>
</tr>
<tr>
<td>Moderate</td>
<td>50 000 – 200 000 SEK</td>
</tr>
<tr>
<td>Minor</td>
<td>1 – 50 000 SEK</td>
</tr>
<tr>
<td>Insignificant</td>
<td>0 SEK</td>
</tr>
</tbody>
</table>

Table 11 Consequence table for the "Customer information"-asset

The consequence scale for the asset “Company information” is shown in Table 12.

<table>
<thead>
<tr>
<th>Consequence value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Integrity</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>100 000+ SEK</td>
</tr>
<tr>
<td>Major</td>
<td>50 000 – 100 000 SEK</td>
</tr>
<tr>
<td>Moderate</td>
<td>25 000 – 50 000 SEK</td>
</tr>
<tr>
<td>Minor</td>
<td>1 – 25 000 SEK</td>
</tr>
<tr>
<td>Insignificant</td>
<td>0 SEK</td>
</tr>
</tbody>
</table>

Table 12 Consequence scale for the "Company information"-asset

Table 13 shows the consequence scale for the asset “Physical server”. For the assets “Physical server” and “WebApp” the consequences are not compromises to information, but rather disturbances in services. If there are disturbances to the physical server which contains the database and the WebApp it results in a loss in time (the time it takes to solve the problem) and money (the loss in income due to one employee, possibly more, working on getting the server back up and running). In this table as well the cost has been calculated in SEK.

<table>
<thead>
<tr>
<th>Consequence value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>7+ days of disturbances</td>
</tr>
<tr>
<td>Major</td>
<td>4-6 days of disturbances</td>
</tr>
<tr>
<td>Moderate</td>
<td>2-3 days of disturbances</td>
</tr>
<tr>
<td>Minor</td>
<td>1 day of disturbances</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No disturbance</td>
</tr>
</tbody>
</table>

Table 13 Consequence scale for the “Physical server”-asset

In Table 14 the consequence scale for the asset “WebApp” is shown.
### Table 14 Consequence scale for the "WebApp"-asset

<table>
<thead>
<tr>
<th>Consequence value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>7+ days of disturbances</td>
</tr>
<tr>
<td></td>
<td>19 200+ SEK</td>
</tr>
<tr>
<td>Major</td>
<td>4-6 days of disturbances</td>
</tr>
<tr>
<td></td>
<td>9 601- 19 200 SEK</td>
</tr>
<tr>
<td>Moderate</td>
<td>2-3 days of disturbances</td>
</tr>
<tr>
<td></td>
<td>3 501- 9 600 SEK</td>
</tr>
<tr>
<td>Minor</td>
<td>1 day of disturbances</td>
</tr>
<tr>
<td></td>
<td>1 – 3 500 SEK</td>
</tr>
<tr>
<td>Insignificant</td>
<td>No disturbance</td>
</tr>
<tr>
<td></td>
<td>0 SEK</td>
</tr>
</tbody>
</table>

The risk evaluation matrix for the “Customer information”, “Company information”, “Physical server” and “WebApp” assets is shown in Table 15. The risk matrix is described by Braber et al [1] as:

> “It has likelihood and consequence values as its axes so that a risk with a specific likelihood and consequence will belong to the intersecting cell.”

When the risk matrices for the assets listed above were created the results were identical, therefore they were reduced to a single matrix, see Table 15.

The green coloured cells containing the word “Acceptable” represent risk situations which are considered acceptable. Red coloured cells containing the phrase “Must be evaluated” represent risk situations which must be evaluated further in the risk analysis.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
</tr>
<tr>
<td></td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
</tr>
<tr>
<td>Possible</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
<tr>
<td></td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
<tr>
<td>Likely</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
<tr>
<td>Certain</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
</tbody>
</table>

Table 15 Risk evaluation matrix for the “Customer information”, “Company information”, “Physical server” and “WebApp” assets.

Table 16 shows the consequence scale defined for the asset “Financial information”.

<table>
<thead>
<tr>
<th>Consequence value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>1 000 000+ SEK</td>
</tr>
<tr>
<td>Integrity</td>
<td>225 000+ SEK</td>
</tr>
<tr>
<td>Availability</td>
<td>50 000+ SEK</td>
</tr>
<tr>
<td>Major</td>
<td>200 000 – 1 000 000 SEK</td>
</tr>
<tr>
<td></td>
<td>112 000 – 225 000 SEK</td>
</tr>
<tr>
<td></td>
<td>25 000 – 50 000 SEK</td>
</tr>
<tr>
<td>Moderate</td>
<td>100 000 – 200 000 SEK</td>
</tr>
<tr>
<td></td>
<td>56 000 – 112 000 SEK</td>
</tr>
<tr>
<td></td>
<td>12 500 – 25 000 SEK</td>
</tr>
<tr>
<td>Minor</td>
<td>1 – 100 000 SEK</td>
</tr>
<tr>
<td></td>
<td>1 – 56 000 SEK</td>
</tr>
<tr>
<td></td>
<td>1 – 12 500 SEK</td>
</tr>
<tr>
<td>Insignificant</td>
<td>0 SEK</td>
</tr>
</tbody>
</table>

Table 16 Consequence scale for the "Financial information"-asset
Table 17 shows the risk evaluation matrix for the asset “Financial information”. Due to the higher costs for the consequences, fewer risk situations are acceptable than there was for the previous assets, as shown in Table 15.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
<tr>
<td>Possible</td>
<td>Acceptable</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
<tr>
<td>Likely</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
<tr>
<td>Certain</td>
<td>Acceptable</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
<td>Must be evaluated</td>
</tr>
</tbody>
</table>

Table 17 Risk evaluation matrix for the “Financial information”-asset

3.4 Risk identification

In the risk identification step of the analysis the purpose is to find as many risks to the system as possible. Ideally, all the risks to the system would be found. By going through the assets of the system one by one, identifying unwanted incidents, threat scenarios, vulnerabilities and threats to the assets a list of existing risks posed to the system will be created. The initial threat diagrams (Figure 3.16 - Figure 3.18), that were created in step 2, will be used in this step. The initial threat diagrams should be further specified and completed with additional scenarios if necessary. This risk identification should be performed in a group, with as much diversity as possible in the groups' views of the system. Since different people, with different roles, view the system in different ways they will also see different threats, vulnerabilities etc.

The starting points for this step are the initial threat diagrams, mentioned above. During a meeting with the CEO and the CTO, as well as the analyst, the existing initial threat diagrams are extended with any and all possible scenarios that the participants can identify. The analyst, who has an outside view of the system, presents possible scenarios that could threaten the system. The other participants can then give their view of the suggested scenario, for example answering the following questions. Is the scenario relevant to this system? Are there safeguards in place for this scenario already? Which weaknesses in the system could the scenario exploit? Obviously not only the analyst proposes scenarios during the meeting, the point of having different participants is to make different views of the system available to the analysis. Each suggested scenario is discussed, and if it is deemed possible, likely or not, the scenario is added to the initial threat diagrams. Thereby the initial threat diagrams are taken from the initial stage to the next stage, to become simply threat diagrams.

Below, the threat diagrams that are the results of this step are presented. Figure 3.20 shows the resulting threat diagram for intentional human threats. The diagram is similar to the initial threat diagram that can be seen in Figure 3.16. There are differences however, the excluded assets are no longer present. The “Breaks into the system”-threat scenario has been replaced with “Copies information from the database” and “Accesses the system”. There are also modifications made to the unwanted incidents.
Figure 3.20 Threat diagram for intentional human threats

Figure 3.21 shows the threat diagram for unintentional human threats. That there are changes from the initial threat diagram is quite apparent. During the meetings held during this step of the risk analysis we realized that there were quite a few more vulnerabilities, which could lead to various threat scenarios, than we initially thought. As a result the unwanted incidents were here also modified and new unwanted incidents were added.
Figure 3.21 Threat diagram for unintentional human threats

Figure 3.22 shows the threat diagram for non-human threats. This diagram has also been modified, more threat scenarios were added and the unwanted incidents were changed to be more precise. Instead of “Compromises the availability of the business system”-incident there are now three different incidents. The three new incidents are basically the original incident divided into three, this was done to create a better view of the risks. In addition to better show how different threat scenarios may cause one unwanted incident which in turn may cause other unwanted incidents.
3.5 Risk estimation

In this step of the analysis, the likelihood and consequence scales (Table 10 - Table 14) and threat diagrams (Figure 3.20– Figure 3.22) are used to create risk estimation diagrams. For each of the threat scenarios, an appropriate value from the likelihood scale is chosen and added to the risk estimation diagrams (before this, the risk estimation diagrams are identical to the threat diagrams). The paths of the scenarios are then followed towards the assets through the unwanted incidents. Since multiple threat scenarios can lead to the same unwanted incident (or other threat scenarios) the subsequent likelihood values of the threat scenarios are summarized for each unwanted incident (or following threat scenario), see Table 18 - Table 23. The resulting values are compared to the likelihood scale to see where they are best suited. The final decision for the likelihood values for the unwanted incidents (and following threat scenarios) is up to the client however. They can choose to raise or lower the value to a likelihood value that may not be the mathematically best suited. The way the client views the incident carries more weight than the calculations. The resulting likelihood value is added to the unwanted incident (or following threat scenario) in the risk estimation diagram. After this, the consequences the unwanted incidents will have on the assets are considered. Each relation between an unwanted incident and an asset is given a consequence value. The value is added to the relation in the risk estimation diagram. See Figure 3.23 – Figure 3.25 for the resulting risk estimation diagrams.

The activities that are mentioned above were performed in a meeting with the CEO, where all the likelihoods and consequence values were discussed for the different entities in the diagrams. The resulting diagrams were then sent to the CTO via e-mail for approval. Again, the more views of the system in the analysis, the more complete the analysis. The CTO proposed a couple of changes to the estimations. These propositions were presented to the CEO by me, the analyst, and discussed and finally accepted with the arguments presented by the CTO. The resulting risk estimations are presented below.

Notice that the unwanted incidents in the diagrams have been given designations, for example: CC1, CI1 and CA1. The designations correspond to the category of the incident. CCx is the designation for incidents that Compromise Confidentiality, CIx is the designation for incidents that Compromise Integrity and CAx is the designation for incidents that Compromise Availability. In the designations “x”
is a unique number/identifier for each unwanted incident in a category. These designations will be used later on to refer to the risk scenarios corresponding to the incidents.

Figure 3.23 shows the risk estimation diagram for intentional human threats.

![Risk estimation diagram for intentional human threats](image)

Table 18 shows the combined likelihood table for unwanted incident CC1: “Compromises the confidentiality of the database”. There are three threat scenarios that can lead to this incident, each has a likelihood of Rare (0-1:10y), which means that they may occur zero to one time over a period of ten years. Summarizing these values gives us a likelihood of zero to three times in ten years (0-3:10y), which lands between Rare (0-1:10y) and Unlikely (2-5:10y). In cooperation with Strödata it is decided that the incident suites best in the Rare category.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Likelihood</th>
<th>Unwanted incident</th>
<th>Combined likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat scenario:</strong> Copies information from database before leaving Strödata</td>
<td>Rare (0-1:10y)</td>
<td>CC1: Compromises the confidentiality of the database</td>
<td>3 * (0-1:10y) = (0-3:10y) =&gt; Rare – Unlikely =&gt; Rare</td>
</tr>
<tr>
<td><strong>Threat scenario:</strong> Copies information from database</td>
<td>Rare (0-1:10y)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat scenario:</strong> Breaks into the system</td>
<td>Rare (0-1:10y)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 18 Combined likelihood table for unwanted incident: CC1

Figure 3.24 shows the risk estimation diagram for unintentional human threats.
Table 19 shows the combined likelihood table for the “The WebApp goes down”-threat scenario and the “The database crashes”-threat scenario. These two scenarios can be caused by one threat scenario, “Physical server goes down”, and vulnerability, “Bugs in the WebApp”. The likelihood value of the causing threat scenario is *Likely (21-49 : 10y)*. The vulnerability in itself has no likelihood, however the likelihood that the resulting threat scenarios are reached due to that vulnerability is *Certain (50+:10y)*. These likelihood values give the result *(71-99+:10y)*, 71 to 99 or more times in ten years, placing the threat scenarios firmly in the *Certain (50+:10y)* category.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Likelihood</th>
<th>Threat scenarios</th>
<th>Combined likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat scenario: Physical server goes down</td>
<td><em>Likely (21-49 : 10y)</em></td>
<td>The WebApp goes down And The database crashes.</td>
<td><em>(21-49:10y) + (50+:10y) = (71-99+:10y)</em> =&gt; <em>Certain</em></td>
</tr>
<tr>
<td>Vulnerability: Bugs in the WebApp</td>
<td><em>Certain (50+:10y)</em></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 19 Combined likelihood table for threat scenarios “The WebApp goes down” and “The database crashes”

Table 20 shows the combined likelihood table for the unwanted incident CA2: “Compromises the availability of the database”. There are three threat scenarios that can lead to this incident and one unwanted incident, the first threat scenario has the likelihood value *Certain (50+1:10y)*, the second threat scenario has the likelihood value *Rare (0-1:10y)* and the third threat scenario has the likelihood value *Possible (6-20:10y)*. The unwanted incident has the likelihood value *Certain (50+:10y)*. Resulting
in the sum of \((106-121+:10y)\), 106 to 121 or more times in ten years. This places the result firmly in the *Certain (50+:10y)* category.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Likelihood</th>
<th>Unwanted incident</th>
<th>Combined likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat scenario: The database crashes</td>
<td><em>Certain (50+:10y)</em></td>
<td>CA2: Compromises the availability of the information in the database</td>
<td>2 * (50+:10y) + (0-1:10y) = (106-121+:10y) =&gt; Certain</td>
</tr>
<tr>
<td>Threat scenario: The database is emptied</td>
<td><em>Rare (0-1:10y)</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat scenario: Changes information inappropriately</td>
<td><em>Possible (6-20:10y)</em></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 20 Combined likelihood table for unwanted incident: CA2

Table 21 shows the combined likelihood table for the unwanted incident CI2: “Compromises the integrity of the information in the database”. There are two threat scenarios and one unwanted incident that can lead to this unwanted incident. The combined likelihood value of these gives the value \((106-120+:10y)\), 106 to 120 or more times in ten years. This places the result quite firmly in the *Certain (50+:10y)* category.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Likelihood</th>
<th>Unwanted incident</th>
<th>Combined likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unwanted incident CA1: Compromises the availability of the WebApp</td>
<td><em>Certain (50+:10y)</em></td>
<td>CI2: Compromises the integrity of the information in the database</td>
<td>2 * (50+:10y) + (6-20:10y) = (106-120+:10y) =&gt; Certain</td>
</tr>
<tr>
<td>Threat scenario: Changes information inappropriately</td>
<td><em>Possible (6-20:10y)</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat scenario: Forgotten details</td>
<td><em>Certain (50+:10y)</em></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 21 Combined likelihood table for unwanted incident: CI2

Figure 3.25 shows the risk estimation diagram for non-human threats.
Table 22 shows the combined likelihood table for the unwanted incident CA4: “Compromises the availability of the information in the database”. There is one threat scenario and two unwanted incidents that can lead to this unwanted incident, all three of which have the likelihood value of Possible (6-20:10y). That gives the combined value (18-60:10y), which lands in the range from Possible (6-20:10y) to Certain (50+:10y). It is decided that the incident suites best in the Likely (21-49:10y) category.

<table>
<thead>
<tr>
<th>Cause</th>
<th>Likelihood</th>
<th>Unwanted incident</th>
<th>Combined likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unwanted incident CA3: Compromises the availability of the physical server</td>
<td>Possible (6-20:10y)</td>
<td>CA4: Compromises the availability of the information in the database</td>
<td>3 * (6-20:10y) = (18-60:10y) =&gt; Possible – Certain =&gt; Likely</td>
</tr>
<tr>
<td>Threat scenario: The database goes down</td>
<td>Possible (6-20:10y)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unwanted incident CA5: Compromises the availability of the WebApp</td>
<td>Possible (6-20:10y)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 22 Combined likelihood table for unwanted incident: CA4

Table 23 shows the combined likelihood value table for the unwanted incident CA5: “Compromises the availability of the WebApp”. There are two threat scenarios and one unwanted incident that can lead to this unwanted incident. The two threat scenarios have the likelihood value of Unlikely (2-5:10y) and the unwanted incident has the likelihood value of Possible (6-20:10y), giving a combined value of (10-30:10y) which is in the range from Possible (6-20:10y) to Likely (21-49:10y). It is decided that the incident suites best in the Possible category.
### 3.6 Risk evaluation

In the risk evaluation step of the analysis, the likelihood values of the unwanted incidents and the consequence values on the relations between unwanted incidents and assets will be placed in the risk evaluation matrixes (Table 15 & Table 17) for each of the asset. If an unwanted incident is placed within a “Must be evaluated”-cell that means that the risk must be evaluated further and a treatment should be identified. The client can change the value of a cell in a matrix from “Must be evaluated” to “Acceptable”, or vice-versa, if they feel that it is (not) necessary to evaluate the risk further. To give a more complete view of the risks, risk diagrams will be created. These risk diagrams are based on the risk evaluation matrixes and the threat diagrams. In the risk diagrams the vulnerabilities, threat scenarios and the unwanted incidents have been consolidated into risk scenarios. These are identified by the unwanted incidents’ designations (CCx, Clx, CAx), that were introduced in section 3.5, and given labels to show whether they are acceptable or need further evaluation.

In preparation for a meeting with the CEO and the subsequent e-mail conversation with the CTO, I (the analyst) prepared the initial risk evaluation matrixes by placing the different unwanted incidents in their corresponding cells in the matrixes. During the meeting with the CEO, the initial risk evaluation matrixes were presented and the CEO was given the chance to modify which cells represented values that needed further investigation. The CEO did not see any cells in need of change and the meeting was concluded. Following the meeting with the CEO, the risk evaluation matrixes were presented to the CTO via e-mail for his approval, which was given without need for change. Since no change was needed, only the approved risk evaluation matrixes are presented below (Table 24 - Table 27). After both the CEO and the CTO had given their approval of the risk evaluation matrixes, I (the analyst) created the risk diagrams, which are shown below. These diagrams were sent to both the CEO and the CTO for a final review. These diagrams were also approved without the need for change.

Table 24 shows the final risk evaluation matrix for the “Customer information”-asset. There are seven unwanted incidents that affect this asset, none of which are placed in “Must be evaluated”-cells.

#### Table 23 Combined likelihood table for unwanted incident: CA5

<table>
<thead>
<tr>
<th>Threat scenario</th>
<th>Likelihood</th>
<th>Unwanted incident</th>
<th>Combined likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unwanted incident</strong> CA3: compromises the availability of the physical server</td>
<td>Possible (6-20:10y)</td>
<td>CA5: Compromises the availability of the WebApp</td>
<td>2 * (2-5:10y) + (6-20:10y) = (10-30:10y) =&gt; Possible – Likely =&gt; Possible</td>
</tr>
<tr>
<td><strong>Threat scenario:</strong> The WebApp goes down</td>
<td>Unlikely (2-5:10y)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat scenario:</strong> There are transmission problems</td>
<td>Unlikely (2-5:10y)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Table 24 Risk evaluation matrix for the "Customer information"-asset

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC1, Cl1</td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC2</td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CA2, Cl2</td>
</tr>
</tbody>
</table>

Table 24 Risk evaluation matrix for the "Customer information"-asset
Table 25 shows the final risk evaluation matrix for the “Company information”-asset. There are seven unwanted incidents that affect this asset as well. Here also, none of the risks need further evaluation.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td>CI1</td>
<td>CC1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC2</td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td>CA4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td>CA2, CI2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 25 Risk evaluation matrix for the "Company information"-asset

Table 26 shows the final risk evaluation matrix for the “WebApp”-asset. There are three unwanted incidents that affect this asset. None of the incidents need to be further evaluated.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CA5</td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CA1</td>
</tr>
</tbody>
</table>

Table 26 Risk evaluation matrix for the "WebApp"-asset

Table 27 shows the final risk evaluation matrix for the “Physical server”-asset. There is only one unwanted incident that affects this asset and it does not require further evaluation.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CA3</td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 27 Risk evaluation matrix for the ”Physical server”-asset

Table 28 shows the final risk evaluation matrix for the “Financial information”-asset. There are seven unwanted incidents that affect this asset and all but one needs further evaluation.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC1, CI1</td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CC2</td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td>CA4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td>CA2, CI2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 28 Risk evaluation matrix for the ”Financial information”-asset

The risk diagrams resulting from the risk evaluation matrixes and the threat diagrams are presented below (see Figure 3.26 - Figure 3.30). These diagrams are a more complete view of the risk evaluation than the matrixes since they include the different threats in addition to the risk scenarios. In the risk diagrams the threat scenarios and the unwanted incidents have been consolidated into risk scenarios.
The designations (CCx, Clx, and CAx) that were introduced in the previous step are used here to identify the risk scenarios corresponding to the unwanted incidents. Each of the risk scenarios which are directly linked to an asset have a “risk evaluation”-value attached to them (Acceptable or Unacceptable), these values correspond to the results from the risk evaluation matrixes.

Figure 3.26 shows the risk diagram for the “Customer information”-asset.

![Risk diagram for the "Customer information"-asset](image)

Figure 3.26 Risk diagram for the "Customer information"-asset

Figure 3.27 shows the risk diagram for the “Company information”-asset.
Figure 3.27 Risk diagram for the “Company information”-asset

Figure 3.28 shows the risk diagram for the “WebApp”-asset.

Figure 3.28 Risk diagram for the "WebApp"-asset

Figure 3.29 shows the risk diagram for the “Physical server”-asset. Looking at the risk diagram for this asset, it is worth mentioning again that neither the firewall or the operating system of the server are within the scope of this risk analysis, neither are any system services that may be present.
Figure 3.29 Risk diagram for the "Physical server"-asset

Figure 3.30 shows the risk diagram for the "Financial information"-asset. Notice how, unlike the others, there are risk scenarios that have the value “Unacceptable” attached to them. These are the scenarios that were placed "in the red” of the risk evaluation matrix and that need to be further evaluated and treated.

3.7 Risk Treatment

The previous step, 3.6 Risk evaluation, showed that several risks are in need of further evaluation. In this step, treatments for these risks are identified. A treatment is a way to reduce a risk, more specifically to reduce the likelihood and/or consequences of the risk.

To achieve this, risk treatment diagrams that are based on the threat diagrams are created. In the risk treatment diagrams the relations between unwanted incidents and assets that are unacceptable are identified by risk icons (Figure 3.3) combined with the designation of the unwanted incident. The risk treatment diagrams also contain treatments (Figure 3.10). Following each risk treatment diagram the identified treatments are explained in further detail. The costs of the treatments or the potential size of the reduction in losses is not discussed in this section of the report. In section 4.2 however, there is
a discussion about the changes in Strödata’s calculated losses due to the risks. The calculated losses for the current system, without any of the treatments, are compared to the calculated losses with the treatments in place. To give a better overview of how the treatments that are identified affect the assets and risk scenarios, treatment overview diagrams will also be created in this step.

In preparation of the meeting with the representatives of Strödata, the analyst created an initial list of treatments for the system. This list was the base of the discussion during a meeting with the CEO and the CTO. During the meeting the list was expanded and the treatments were placed in the threat diagrams, where they would be of use. Again, the focus on having different views of the system present at the meeting proved useful. All participants in the meeting had treatments to suggest and define. Once the ideas for treatments ran dry, the analyst took the list and the temporary diagrams and used them to create the risk treatment diagrams below. As well as the explanations of the treatments that are presented after each risk treatment diagram. Treatment overview diagrams were also created by the analyst to give a better overview of how the treatments affect the system, the treatment overview diagrams are presented below. Once these output entities were finished, they were sent to both the CEO and the CTO for approval. All entities were approved without need for changes.

Figure 3.31 shows the risk treatment diagram for intentional human threats. There are two risk icons on the relations between unwanted incidents and the “Financial information”-asset. These are the risks that have been deemed unacceptable for intentional human threats. Also notice the three treatments in the diagram:

- Revise policies
- Analyze user behaviour
- Keep security up-to-date

![Figure 3.31 Risk treatment diagram for intentional human threats](image-url)
"Revise policies" is the first treatment, it affects the "Insufficient policies" vulnerability. Keep the policies up-to-date, make sure the policies cover the areas they should and revise them when the situation changes. The policies should be revised on a regular basis, whether the situation changes or not. To give an example of what the policies should contain: Regulations on how to handle employee user accounts in the business system when an employee leaves the company. Generally there is a three month period when the employee has resigned but still works for the company, consider if the employee should be monitored during this time period or perhaps if these three months should be a paid leave of absence. These regulations should be in place to make sure that leaving employees do not take important (possibly secret) information with them to their new job and thereby causing a loss to the client. In small companies it is not unusual that administrator passwords are common knowledge in the company. By restricting the amount of information each employee has access to, the consequence of an employee changing or taking that information to a competitor is reduced. This security measure is completely void if all the employees in the company know the administrator password to the business system and/or database. This would leave the door to the system wide open and allow employees to access to any information in the system. Information they should not have access to as well as information they should have and/or need access to. Another example of what the policies should contain is regulations about when and how equipment and applications should be updated and patched (this treatment affects future "Update the WebApp"-treatments).

"Analyse user behaviour" is the next treatment, it affects the unwanted incidents CC1 and CI1. Install an intrusion detection system to monitor and analyse user behaviour, and to send out alerts to appropriate people within the company if the activities of a user account deviate too much from the normal pattern. For example: The user account accesses information he/she normally would not access and has no need to access at that time. This would include trying to access resources which are disallowed, for example administrator pages or customer data. This approach has good potential in a system where the users perform the same tasks often, with little deviation. However it can be circumvented through gradually changing the template for the target users’ "normal" behaviour. It takes time but it may not be detected. One strongly deviant action would be noticed but a hundred small deviations may be considered normal. This treatment will most likely be quite hard to set up properly, the restrictions cannot be set too harshly or there will be too many false-positive alerts, if the restrictions are set too loosely it will result in false-negatives. False-positive means that there is an alert caused by normal user activity, false-negative means that there is no alert to deviant user behaviour.

"Keep security up-to-date" is the final treatment suggestion for intentional human threats. The treatment affects the "Insufficient security" vulnerability. Keep the security measures that are in place up-to-date with the latest features and patches to prevent exploitation of known, and fixed, vulnerabilities in the security measures.

Figure 3.32 shows the risk treatment diagram for unintentional human threats. There are three risk scenarios that are deemed unacceptable here and five treatments have been identified.

Treatments for unintentional human threats (each treatment is explained further below):

- Extend training, increase focus on security
- Update the WebApp
- Revise policies
- Separate the production and lab environments
- Access business system from smartphone

Figure 3.32 Risk treatment diagram for unintentional human threats

There are two instances of the “Extend training, increase focus on security” treatment. The reason for this is that the extended training affects both the “Insufficient training” vulnerability and the “Carelessness” vulnerability. How the treatment affects the “Insufficient training” vulnerability should be obvious, more training results in fewer mistakes due to lack of knowledge. As for carelessness, it can be a result of different things. It can be due to the employees’ lack of knowledge about possible consequences. Carelessness may also be a result of the employee not caring about the possible consequences or not caring enough to look over the input to make sure it is correct. In any case, further training is a suitable treatment.

The second treatment, “Update the WebApp”, affects the vulnerability “Bugs in the WebApp”. Update the WebApp to make it more robust. Meaning that it should take more for the WebApp to go down or
cause unintended changes than it does today. This can be achieved by updating it to a newer (well tested) stable technology and/or patching known bugs. While doing this the performance of the WebApp may increase as well, giving some additional incitement.

"Revise policies" is the third treatment, it affects the “Insufficient policies” vulnerability. The reasoning behind it here is the same as for intentional threats above.

The "Separate the production and lab environments" treatment affects the "Production and lab environment on the same physical server" vulnerability. By separating these two environments to two machines, the likelihood that the physical server goes down, due to activities in the lab environment, and brings the production system with it, decreases. By decreasing this likelihood, the likelihood that the WebApp and database become unavailable also decreases.

"Access business system from smartphones" is the final treatment for unintentional threats. It affects the “Insufficient availability of the business system”. To prevent details from being forgotten, there must be ways to submit information to the system at any time, preferably just after an activity is finished. One way to accomplish this is to enable access to the business system through smartphones. The way the system is implemented at the time of writing (March 2011), access from smartphones is not a valid option. The system is not adapted for it. Accessing the system from smartphones also provides new and interesting possibilities. However, this treatment in itself presents new risks, more on this in section 4.1 of this report.

Figure 3.33 shows the risk treatment diagram for non-human threats. There is one risk scenario that is deemed unacceptable and two treatments.

Treatments for non-human threats (each treatment is explained further below):

- Virtualize the server
- Update the WebApp
Figure 3.33 Risk treatment diagram for non-human threats

The first treatment, “Virtualize the server”, affects the unwanted incident “Compromises the availability of the physical server” and the risk scenario “The physical server goes down”. Using a virtual server instead of a physical one allows for better disaster recovery, as described by Mah [5]. Since the server itself is only a file stored on a machine a backup can be copied to another machine and be up and running again within a short period of time. A virtual server can be run on any machine that has the virtualization software, the hardware configuration is not very important. If the hardware that the server is running on goes down for some reason the server can be moved to (more or less) any other machine that still functions. Without the virtualization this would not be possible, there would need to be a, if not identical, very similar machine at hand to take over the duties of the malfunctioning server. The point is that the server would have less downtime if the physical server is not functioning for a longer period of time than it takes to start up the virtual server on another machine.

The second treatment, “Update the WebApp”, affects the risk scenario “The WebApp goes down”. The reasoning behind it here is the same as for the unintentional threats above.

To give an overview of how the different treatments that have been identified affect the assets and risk scenarios, treatment overview diagrams are created. Below, these diagrams are presented (see Figure 3.34 - Figure 3.38). The treatment overview diagrams are based on the risk diagrams, with the addition of the treatments.

Figure 3.34 shows the treatment overview diagram for the “Customer information”-asset.
Figure 3.35 shows the treatment overview diagram for the "Company information"-asset.

Figure 3.36 shows the treatment overview diagram for the "Financial information"-asset.
Figure 3.36 Treatment overview diagram for the "Financial information"-asset

Figure 3.37 shows the treatment overview diagram for the "WebApp"-asset.

Figure 3.37 Treatment overview diagram for the "WebApp"-asset

Figure 3.38 shows the treatment overview diagram for the "Physical server"-asset.
Figure 3.38 Treatment overview diagram for the "Physical server"-asset
4 Analysis
This section of the report contains an analysis of the risk analysis itself. How access to the business system from a smartphone would affect the risks (less/more risks, new risks, eliminated risks etc.) will be discussed. This section will also contain a resulting view of the system if/when all the treatments are implemented. A comparison between calculated losses before and after the treatments are implemented will be shown as well. Finally there will be a section discussing what the risk analysis showed.

Since one of the main reasons for this thesis project is to enable access to Strödata’s web based business system through smartphones the first sub-section focuses on how the risks posed to the system will be affected by enabling this access.

4.1 Accessing the business system from a smartphone
How would accessing the business system from a smartphone affect the risks? Enabling access to even a small part of the system, such as the work reporting part, may result in unacceptable risks. How would Strödata’s system be affected if it was possible to perform the work reporting task from a smartphone?

Reporting work from a smartphone is the next logical step following the introduction of a web-based business system, and the possibility to do so would lower the probability of employees inserting erroneous information into the system because they do not remember the details correctly. The shorter the time span between performing the assignment and creating the work report, the higher the quality of the report. The larger the time span, the larger the probability that details are forgotten or remembered incorrectly. For example: not remembering the amount of time the assignment actually took may cause a loss of income. Probably not a large loss on each occasion, but if it occurs enough times the amount will build up.

A precondition to create work reports from a smartphone, or to access the business system at all from a smartphone, is that the smartphone has a connection to the internet. A smartphone’s internet access is provided by the telephone network operator. For the smartphone access to the business system to make sense, we must assume that the employees’ smartphones have that internet access. The telephone network providers help us strengthen this assumption with their coverage maps. Strödata is a company based in Skåne, this is also where Strödata’s customers are located. The figures (Figure 4.1 - Figure 4.4) below show four of the major telephone network providers’ coverage maps. The small map-pin in each of the maps shows the location of Vinslöv, where one of Strödata’s offices is located. The coverage maps present the telephone network providers data-traffic (internet access) coverage of their third generation networks and earlier. The fourth generation data-traffic coverage is omitted since it is only implemented in small parts of the country at the time of writing, and the older generations are sufficient to access the business system. Figure 4.1 shows the telephone network provider Tele2’s data-traffic coverage (third generation and older). Included in the figure is the legend of the colours used in the coverage map. The coverage map shows that the entirety of Skåne is covered.
Figure 4.1 Tele2 coverage map

Figure 4.2 shows the telephone network provider Telenor’s data-traffic coverage (third generation and older). Included in the figure is the legend of the colours used in the coverage map. The coverage map shows that the entirety of Skåne is covered.

Figure 4.2 Telenor coverage map

Figure 4.3 shows the telephone network provider Telia’s data-traffic coverage (third generation and older). Included in the figure is the legend of the colours used in the coverage map. The coverage map shows that the entirety of Skåne is covered.

Figure 4.3 Telia coverage map

1 https://www.telia.se/privat/mobilt/mer-om-mobiltelefoni/tackning-hastighet/tackning-mobiltelefoni/tackning-mobiltelefoni_new.page
2 http://www.telenor.se/privat/kundservice/tackning-och-driftinfo/tackning/tackningskarta.html
3 http://www.tre.se/Privat/Kundservice/Tackning-drift/Tackningskarta/
Figure 4.4 shows the telephone network provider Tre’s data-traffic coverage (third generation and older). Included in the figure is the legend of the colours used in the coverage map. The coverage map shows that the entirety of Skåne is covered.

The data-traffic coverage maps, presented above, all show that the data-traffic coverage from the telephone network providers covers very close to the entirety of Skåne. My personal experience, however, is different. There are places where one or several of the telephone network providers have low or no coverage for data-traffic as well as voice-calls. These places are usually not located where companies (and possible customers for Strödata) are located.

The consequences that lack of data-traffic coverage would have for the smartphone access to the business system through smartphones would be the same situation as not having that access available at all. In other words, it would be the same situation as the present. The employees would have to find internet access some other way or at some other location, which would make it probable that they would wait to create work reports until they are back at one of the offices. However, considering the coverage maps presented by the telephone network providers that are shown above, this situation will not be a common one, making the risk it presents negligible.

Part of this thesis project is to develop a web application with the purpose of enabling the creation of work reports from smartphones, therefore it is of interest to see how that action would affect the risks posed to the system. If the analysis shows that the consequences are greater than the benefits, the application should not be put to use. Even if the risks are not too large, knowing the risks will hopefully lead to better understanding and better use of the application.

Below follows a high-level analysis of how work reporting through a smartphone would affect the risks posed to Strödata’s business system. The high-level analysis was performed during a meeting between the CEO and CTO of Strödata and myself, the analyst. During the meeting we discussed how smartphone access to the business system would affect the risk posed to the system at present. We looked over the threat diagrams that are presented in section 3.4, see Figure 3.20 - Figure 3.22, and pointed out where smartphone access might affect the system. We also looked over the suggested treatments that are presented in section 3.7 and re-established that smartphone access is a treatment for the “Insufficient availability of the business system”-vulnerability. During the meeting we also

4 https://www.tele2.se/kundservice/drift-och-tackning/tackningskarta.aspx
created new risk scenarios regarding smartphone access. After the meeting I created a new threat diagram for intentional human threats that only contains the risk scenarios relating to the smartphone access. I also created an isolated treatment diagram for the vulnerability “Insufficient availability of the business system”, where smartphone access to the business system is identified as a treatment. Both diagrams are presented below. The diagrams were sent to the CEO and the CTO for approval, which was given without need for changes.

By introducing a way to access the business system through a smartphone the risks to the system will change. The reason for accessing the business system from smartphones is the increased mobility of the business system. It can be accessed from anywhere, as opposed to the current state which requires a computer with an internet connection. The smartphone always has the internet connection (how the connection works and how it is paid for depends on the deal with the carrier). The fact that most people always have their smartphones with them is another factor when it comes to mobility. Since the smartphone is always at hand, accessing the business system is possible at all times. However, the fact that smartphones are a rather attractive target for thieves combined with their small size make them rather easy to lose. If a thief stole a smartphone with some kind of access to Strödata’s business system the thief could gain access to the system if the user credentials are saved on the phone. This could happen if the phone has an application specifically designed for accessing the business system or a bookmark to the business systems web-page. If the user credentials are not saved on the phone it will have little effect if the thief has access to an interface to the business system or not since he/she cannot get inside the system without proper credentials. If user credentials are saved on the smartphone, that may lead to two previously defined threat scenarios and the corresponding unwanted incidents.

There is also the possibility of spyware applications, applications that record what the user does and sees. Since such an application could be running on any employees smartphone, recording everything that the employee does, from entering their passwords to the information that is returned from Strödata’s database. The application could then send the gathered information to an attacker. The result being access to Strödata’s database through recorded user credentials, or parts of the database that have been sent to the user. For example: the list of customers an employee has to choose from when performing a work report. This also leads to an already existing threat scenario, where a hacker copies information from Strödata’s database.

The threat scenarios that are described above are shown in Figure 4.5.
Figure 4.5 Threat diagram for intentional human threats for smartphones

Allowing smartphones to access the business system does not only result in new risks but also a treatment for the vulnerability “Insufficient availability of the business system”, see the treatments for unintentional human threats in section 3.7. Being able to access the business system and report work from a smartphone more or less eliminates this vulnerability and the consequences it may yield. Figure 4.6 shows the part of the treatment diagram for unintentional human threats (Figure 3.32) which deals with this treatment and this situation.

Figure 4.6 Part of the treatment diagram for unintentional human threats for smartphones

Allowing smartphones to access the business system to report work also provides some interesting ways to develop the business system further. For example: When an employee is done (earlier than expected) with an assignment and reports the work through a smartphone. The system can select the next job site for the employee automatically, using a priority-list of jobs together with the location of the employee (a GPS device is included in most, if not all, smartphones. Even if the smartphone has no GPS device there may be other location services and then is the possibility of triangulating the position based on phone network base stations). This would enable the employee to go to a highly prioritized job that is close to the previous job-site, without going back to the office. Even a map and directions could be provided.
4.2 Resulting system view

Given that the treatments that are suggested in section 3.7 of this report are implemented, even just one, the result will be changes to the risks posed to the system. This section of the report will show a resulting view of the system where all the treatments are implemented. Be sure to note that among the treatments is “Access business system from smartphone” which not only is a treatment but also introduces new risks. The resulting view of the risks will show how the risks would change. Some risks may disappear, others may be added, yet others may have their consequences or likelihoods changed. The changes will be shown in risk estimation diagrams. For comparison, the original risk estimation diagrams will be shown again, following the resulting risk evaluation diagrams. New risk evaluation matrixes will be created from the resulting risk evaluation diagrams, to help illustrate the changes.

As a result of these changes, the losses that the risks/threats/incidents cause will change as well. These changes will be calculated and the results will be shown in tables and compared to the calculated losses without the treatments.

The changes to the system and the calculations that were performed as a cause of the changes were performed during a meeting between the CEO and myself, the analyst. During the meeting we discussed how each treatment affected the system and to what extent it would reduce its’ associated risk. The likelihood scale, Table 10, and the consequence tables, Table 11 - Table 14, were used as a reference when discussing the changes. During the meeting we noted the changes to the likelihood and consequence values, these notes were later used to create the change tables that are presented below. As well as the resulting risk estimation diagrams, those are also presented below together with original risk estimation diagrams. Furthermore, the change tables were also used to update the risk evaluation matrixes to create the resulting risk evaluation matrixes that are presented below. Finally the change tables were used to create the table containing the changes in calculated losses, also presented below. All these outputs were presented to the CEO and the CTO for approval. They were all approved without need for changes.

One of the changes to the intentional threats is the “Thief”-threat and the following risks. The threat is a result of enabling access to the system through smartphones. A smartphone is a mobile device (which is the point of the smartphone access to the system) and thereby it is quite easy to steal. If the employee has his user credentials saved on the phone the thief has access to the system. Another change is the threat scenario where a “Hacker”-threat uses a spyware application to gather information, from the database or perhaps user credentials which may lead to unauthorized access to the system. This is also a result of enabling access to the system through smartphones.

To show the difference between the resulting risks (including treatments) and the original risks (without any treatments implemented), Figure 4.7 shows the risk estimation diagram for intentional threats before the treatments or smartphone access have been implemented. Notice that there are some duplicate entities in the resulting risk estimation diagram, see Figure 4.8. The reason for duplicate entities is to clarify the changes caused by new threats. Of the duplicates, one is from the original risk estimation diagram and the other is a result of enabling smartphone access to the business system (as discussed in the previous section of the report, section 4.1). Red rectangles have been added to the resulting risk estimation diagrams to highlight the changes.
Figure 4.7 Risk estimation diagram for intentional human threats

Figure 4.8 Resulting risk estimation diagram for intentional threats

The likelihood values for the risks and unwanted incidents have not changed here. The new risks that have been added due to the implementation of the treatments have all been estimated to the lowest possible likelihood value, Rare (0-1:10y). When representatives of the client look back there has been no thefts of employee smartphones since they were introduced in the company. And while mobile malware is on the rise at the time of this analysis (March 2011) [15, 16, 17], representatives from...
Strödata felt that within the company it is still rare. However two of the consequences for the “Financial information”-asset have changed. This is mainly due to the treatment “Analyse user behaviour” which the CEO and the CTO felt reduced the possible consequences quite a bit, as can be seen in Table 29 where the changes are shown.

<table>
<thead>
<tr>
<th>Unwanted incident</th>
<th>Old consequence</th>
<th>New consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
<td>Major (200 000 – 1 000 000 SEK)</td>
<td>Moderate (100 000 – 200 000 SEK)</td>
</tr>
<tr>
<td>CI1</td>
<td>Catastrophic (225 000+ SEK)</td>
<td>Major (112 000 – 225 000 SEK)</td>
</tr>
</tbody>
</table>

Table 29 Consequence changes for the “Financial information”-asset and intentional threats

Two large changes to the resulting risk estimation diagram for unintentional threats, Figure 4.10, are the removal of the vulnerabilities “Production and lab environments on the same physical server” and “Insufficient availability of the business system”, as well as the threat scenarios they result in. The vulnerabilities and the threat scenarios are removed due to the treatments that affect them.

To show the difference between the resulting risks (including treatments) and the original risks (without any treatments implemented), Figure 4.9 shows the risk estimation diagram for intentional threats before the treatments were implemented.

![Risk estimation diagram for unintentional human threats](image-url)
All but one likelihood value for the threat scenarios and unwanted incidents have been changed because of the treatments. The changes to the threat scenario likelihood values are shown in Table 30.

<table>
<thead>
<tr>
<th>Threat scenario</th>
<th>Old likelihood value</th>
<th>New likelihood value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The WebApp goes down</td>
<td>Certain (50+:10y)</td>
<td>Unlikely (2:5:10y)</td>
</tr>
<tr>
<td>The database crashes</td>
<td>Certain (50+:10y)</td>
<td>Unlikely (2:5:10y)</td>
</tr>
<tr>
<td>Changes information inappropriately</td>
<td>Possible (6-20:10y)</td>
<td>Rare (0-1:10y)</td>
</tr>
<tr>
<td>Accesses information inappropriately</td>
<td>Possible (6-20:10y)</td>
<td>Rare (0-1:10y)</td>
</tr>
</tbody>
</table>

Table 30 Likelihood changes for threat scenarios for unintentional threats

The changes to the unwanted incidents likelihood values are shown in Table 31.
Table 3.1 Likelihood changes for unwanted incidents for unintentional threats

For the non-human threats the only changes are to the likelihood values for the threat scenarios and unwanted incidents, see Figure 4.12.

To show the difference between the resulting risks (including treatments) and the original risks (without any treatments implemented), small as they may be, Figure 4.11 shows the risk estimation diagram for intentional threats before the treatments were implemented.

Figure 4.11 Risk estimation diagram for non-human threats
Figure 4.12 Resulting risk estimation diagram for non-human threats

Table 32 and Table 33 show the changes to the likelihood values for threat scenarios and unwanted incidents regarding non-human threats.

<table>
<thead>
<tr>
<th>Threat scenario</th>
<th>Old likelihood value</th>
<th>New likelihood value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The physical server crashes</td>
<td>Certain (50+:10y)</td>
<td>Possible (6-20:10y)</td>
</tr>
<tr>
<td>The WebApp goes down</td>
<td>Unlikely (2-5:10y)</td>
<td>Rare (0-1:10y)</td>
</tr>
</tbody>
</table>

Table 32 Likelihood changes for threat scenarios for non-human threats

<table>
<thead>
<tr>
<th>Unwanted incident</th>
<th>Old likelihood value</th>
<th>New likelihood value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA3</td>
<td>Possible (6-20:10y)</td>
<td>Unlikely (2-5:10y)</td>
</tr>
</tbody>
</table>

Table 33 Likelihood changes for unwanted incidents for non-human threats

To show the effect that the treatments have on the system as clearly as possible, the resulting risk estimation matrixes are presented below, see Table 34 - Table 38.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unlikely</td>
<td>CI2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Possible</td>
<td>CA2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Likely</td>
<td>CA4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 34 Resulting risk evaluation matrix for the “Customer information”-asset
Consequence | Insignificant | Minor | Moderate | Major | Catastrophic
---|---|---|---|---|---
Frequency | Rare | CI1 | CC1 | CC2 |  
Unlikely | CI2 |  
Possible | CA2 |  
Likely | CA4 |  
Certain |  |  
Table 35 Resulting risk evaluation matrix for the “Company information”-asset

Consequence | Insignificant | Minor | Moderate | Major | Catastrophic
---|---|---|---|---|---
Frequency | Rare |  |  |  |  
Unlikely | CA1 |  
Possible | CA5 |  
Likely |  |  
Certain |  |  
Table 36 Resulting risk evaluation matrix for the “WebApp”-asset

Consequence | Insignificant | Minor | Moderate | Major | Catastrophic
---|---|---|---|---|---
Frequency | Rare |  |  |  |  
Unlikely | CA3 |  
Possible |  |  
Likely | CA4 |  
Certain |  |  
Table 37 Resulting risk evaluation matrix for the “Physical server”-asset

Consequence | Insignificant | Minor | Moderate | Major | Catastrophic
---|---|---|---|---|---
Frequency | Rare | CC1 | CI1 | CC2 |  
Unlikely | CI2 |  
Possible | CA2 |  
Likely | CA4 |  
Certain |  |  
Table 38 Resulting risk evaluation matrix for the “Financial information”-asset

Since the “Financial information”-asset is the asset with the most scenarios that need further evaluation, the final risk evaluation matrix for the asset is shown below for comparison, see Table 39.

Consequence | Insignificant | Minor | Moderate | Major | Catastrophic
---|---|---|---|---|---
Frequency | Rare | CC1 | CI1 | CC2 |  
Unlikely |  |  
Possible | CC2 |  
Likely | CA2 |  
Certain | CA4 |  
Table 39 Risk evaluation matrix for the “Financial information”-asset

It is clear that all the scenarios have not been treated enough to reach acceptable levels. It is also clear that the risk for all but one scenario has been reduced, either the frequency at which they occur has been reduced or the resulting consequence. More on this in following section of the report (section 4.3 What did the risk analysis show?).
Since the likelihood values of the incidents and the consequences the incidents have on the assets have changed, so has the calculated loss for these incidents. Table 40 shows how the calculated losses have changed between a situation with no treatments implemented and a situation where all the suggested treatments have been implemented.

<table>
<thead>
<tr>
<th>Risk scenario</th>
<th>Calculated loss over a 10 year period, without treatments implemented</th>
<th>Calculated loss over a 10 year period, with treatments implemented</th>
<th>Difference in losses over a period of 10 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC1</td>
<td>0 – 2 100 000 SEK</td>
<td>0 – 1 300 000 SEK</td>
<td>Reduction by: 0 – 800 000 SEK</td>
</tr>
<tr>
<td>CC2</td>
<td>4 200 000 – 10 500 000+ SEK</td>
<td>0 – 2 100 000+ SEK</td>
<td>Reduction by: 4 200 000 – 8 400 000 SEK</td>
</tr>
<tr>
<td>CI1</td>
<td>0 – 277 500+ SEK</td>
<td>0 – 277 500 SEK</td>
<td>Reduction by: 0+ SEK</td>
</tr>
<tr>
<td>CI2</td>
<td>2 800 100 – 6 275 000+ SEK</td>
<td>25 004 – 160 000 SEK</td>
<td>Reduction by: 2 775 096 – 6 115 000 SEK</td>
</tr>
<tr>
<td>CA1</td>
<td>50 – 175 000+ SEK</td>
<td>2 – 17 500 SEK</td>
<td>Reduction by: 48 – 157 500+ SEK</td>
</tr>
<tr>
<td>CA2</td>
<td>150 – 975 000+ SEK</td>
<td>18 – 390 000 SEK</td>
<td>Reduction by: 132 – 585 000+ SEK</td>
</tr>
<tr>
<td>CA3</td>
<td>6 – 70 000 SEK</td>
<td>2 – 17 500 SEK</td>
<td>Reduction by: 4 – 52 500 SEK</td>
</tr>
<tr>
<td>CA4</td>
<td>63 – 955 500 SEK</td>
<td>63 – 955 500 SEK</td>
<td>No change</td>
</tr>
<tr>
<td>CA5</td>
<td>6 – 70 000 SEK</td>
<td>6 – 70 000 SEK</td>
<td>No change</td>
</tr>
</tbody>
</table>

Table 40 Changes in calculated losses with and without treatments

As you can see there are some quite large differences over a ten year period. There are also risk scenarios where the calculated loss has not changed and one scenario where the reduction in losses is “0+ SEK”. The value “0+ SEK” is due to the fact that without treatments the scenario reached the “Catastrophic” consequence level, where the cost is “from 277 500 SEK and up”. The reduction would then be however much higher than 277 500 SEK the loss would have reached.

The total calculated difference in losses is a reduction by 6 975 280 – 16 110 000+ SEK.

The exact amount depends on how much over the catastrophic values the losses are. The calculated reduction is at least 6 975 280 SEK over a ten year period.

The calculated reduction in losses could be seen as the amount of money the treatments are allowed to cost (to not cause a loss when purchased). Should the treatments cost less, all the better.

4.3 What did the risk analysis show?
This section of the report will deal with the results of the risk analysis. The goal is to answer the questions:

- What did the analysis actually show?
- What risks are still present in the system and can they be treated?
- Are the identified treatments enough to reduce the risks to acceptable values?
- Is smartphone access to the business system a good idea?

The risk analysis showed that there are risks to Strödata’s business system, as there are to any other system. Some of the risks are within the acceptable limits that have been established, others are not. All the unacceptable risks can be treated, and treatments have been identified. These treatments will reduce the risks and in some cases eliminate them.

As the resulting view of the system shows in section 4.2, the risks will be reduced and some eliminated. For the risks that are reduced but not eliminated, not all of the risks reach all the way to acceptable levels. This shows that there is need for further treatments and/or a revision of the acceptability limits of the risks.

As the risks are reduced through the treatments that were identified in section 3.7, the result will be a reduction in losses for Strödata. The size of this reduction is by no means insignificant. However, the size of the reduction is not a single constant value, it is an approximate range. Due to how the consequence values have been defined, as a range of SEK (for example: for the “Company information”-asset the consequence value for a compromise to the confidentiality of the information to the Major level. The consequence value is “50 000 – 100 000 SEK”) the resulting reduction in losses is also a range. The difference between the lowest and the “highest” value of the reduction in losses is almost 9 000 000 SEK. This difference may be even greater, the “highest” value may be even larger. Also due to how the consequence values are defined, the “highest” value is not a constant. For example: The Catastrophic value for the asset “Company information”-asset and a compromise of the confidentiality of the information has the consequence value “100 000+ SEK”. Which means that the consequence has a value greater than 100 000 SEK, how much greater depends on the compromise. Since the values may be greater than the “highest” value (100 000 SEK), the resulting reduction in losses varies in the same way.

If we ignore that the value of the reduction in losses is not an exact, single and constant value. It can be used as an incentive to finance the treatments. The reduction can be viewed as the available cost for the treatments. If the cost to implement the treatments is greater than the reduction in losses they would result in, perhaps they should not be implemented. Perhaps only implement a part of the identified treatments, those that deemed to be the most cost effective. Another alternative is to attempt to identify other, cheaper, treatments.

Keeping this in mind, the question is if smartphone access to the business system is a good idea or not? The answer: it probably is. The risks that are introduced as a result of smartphone access are not severe enough to outweigh the benefits. Generally speaking, most people are careful not to lose their smartphone. Not only because of the cost to replace a lost smartphone, but it is also because of the amount of personal and professional information that is stored on them. To further increase the care the employees at Strödata have for their smartphones, it is a good idea to add some more weight to the problems that may be caused by a lost or stolen smartphone in the training the employees receive. Such things as “Don’t leave the smartphone on the coffee shop table when you go to the restroom” and “Don’t save user credentials on the smartphone” may be good points to mention in the training, if smartphone access is enabled for the system.
Considering the threat of spy-software on the employee’s smartphones, this threat is already present in connection to the employees’ computers. Computers however are generally better protected than smartphones, even if antivirus software for smartphones is starting to emerge at the time of writing. Awareness about spy-software for both smartphones and computers should also be addressed in the training employees receive.

Limiting the access to the business system from smartphones may also be a good idea. Only allow certain features to be accessed from the smartphone, for example: work reporting and work priority lists. Having access to the business system through a smartphone opens up a large wealth of possible features that are not present in the business system today. For example: a start-finish time feature. When the employee starts to move to a client from the office he/she starts the feature. This starts a time-counter and a distance-counter. When the employee is finished with the work for the client he/she stops the feature and is presented with a work reporting form, with time spent at the client as well as distance travelled provided.

Access to the business system through smartphones undoubtedly opens up exciting possibilities but it also creates new risks. The new risks should not be ignored or forgotten, they need to be addressed. There are however ways to mitigate them, mainly through education. User behaviour plays a great roll in many risks to the system. Something as simple as being aware of the risks that smartphone access creates can help reduce the negative impact the access may have.
5 The Application

This section of the report is dedicated to the application that shall be developed as part of this thesis project. The applications purpose will be to enable work reporting to be performed from a smartphone. A use case, based on the case presented in section 2, is presented below in section 5.2. How to achieve the purpose of the new application is a matter of choice, in section 5.1 several suggestions are presented. Each suggestion will include pros and cons for that solution. These suggestions are presented to representatives from Strödata who will decide which suggestion shall be developed.

Section 5.3 presents the chosen solution in a more detailed description. This section will contain information about why this solution was selected, how it will be implemented (what languages and frameworks will be used) as well as instructions on how to use the application.

Section 5.4 describes how a demonstration of the proof-of-concept application was performed, as well as the feedback from the representatives from Strödata after the demonstration.

5.1 Suggested solutions

In this section of the report five possible solutions to achieve the goal will be presented.

At the start of this project thesis the idea for the application that is to be developed was to create an Android application that enabled access to the business system. This was only an initial idea and not very detailed or discussed. It was understood that creating an Android application that contained all of the features that the current business system has might be too large of a project to be contained in this project thesis. It was therefore decided that if the development proved to be arduous, a proof-of-concept application should be implemented instead of implementing all of the features of the current business system. The proof-of-concept application would be limited to the activity of creating work reports.

As my understanding of the current system progressed in parallel with the progress of the risk analysis of the current system, in particular when the “Insufficient availability of the business system”-vulnerability was identified, my view of how the proof-of-concept application should be implemented changed. All the employees working at Strödata have smartphones, but not all employees have Android smartphones. Both iPhone and Windows smartphones were represented within the company. If the proof-of-concept application was developed only for Android, these employees would still suffer from the above mentioned vulnerability in the same manner as they currently do. The question as to how all the employees could access the business system through their various smartphones was raised. One solution is to develop several applications, one for each smartphone operating system. Another would be to develop a cross-platform application. Using the existing system was also considered, simply accessing it through the smartphone (via internet browser or an application displaying a webview). After an exploratory testing session, this solution was abandoned. The web page is designed for computer-sized screens and therefore there are a number of problems (tables and text overlapping among other things) that makes this option unfeasible.

Discussions on this matter were conducted sporadically during the risk analysis part of this project thesis. As the risk analysis part of the project was nearing its end, these discussions became more necessary and more urgent. To resolve this matter a meeting between the CEO, the CTO and I, as the analyst during the risk analysis and developer of the proof-of-concept application, was held. The initial
idea of an Android application was discussed and the problems mentioned above. We also discussed other possible solutions, for example implementing applications for several operating systems. That particular solution was discarded because of the amount of time and work it would require. Another proposed solution was to implement a new web-application based on the current system. The new web-application proof-of-concept would be better adapted for the use on smaller screens. Several other suggestions were proposed (and discarded) during this meeting and several sporadic discussions between the meeting participants following the meeting. During the following sporadic discussions regarding the possible solutions other employees at Strödata were also involved, however they did not always participate. As a result of the meeting and the following discussions a list of possible solutions was created and updated as needed when new arguments arose. The final list of suggested solutions is presented below.

In the sections below a number of suggestions for solutions are presented. Each of the suggestions contain a short description, a list of pros (bullet point: +) and cons (bullet point: -) for that solution as well as a list of notes (bullet point: *).

### 5.1.1 Adapted WebApp GUI 1
Access the business system through an adaptation of the existing WebApp using the smartphone’s web browser.

+ Platform independent, can be accessed through any browser on any smartphone (assuming they have support for SSL and certificates).
+ Will contain most (if not all) functionality of the business system, depending on how much work is required to adapt the existing web application.
+ The GUI of the WebApp will be adapted for smaller screens.
- Requires trust in the smartphone’s web browser. Since Strödata has no control over the browser, or the code it runs.
* High re-use. Much of the system can be re-used.
* Medium to high amount of work required to adapt the GUI of the WebApp.

### 5.1.2 Adapted WebApp GUI 2
Access the business system through an adaptation of the existing WebApp using an Android application.

+ Will contain most (if not all) functionality of the business system, depending on how much work is required to adapt the existing web application.
+ Strödata has control over the application and its code.
+ The GUI of the application will be adapted for smaller screens.
- Generally not good practice to create an application which only shows a web page.
* High re-use. Much of the system can be re-used.
* Medium to high amount of work required to adapt the GUI of the WebApp and implement the Android application.

### 5.1.3 Rebuild 1
Access the business system through a new web service using an Android application.
Strödata has a large measure of control over both the application and the web service and their code.

The GUI of the application will be adapted for smaller screens.

Good possibilities for further development.

- Limited functionality of the application (limited to the original idea of work reporting). Depending on how difficult and time-consuming the implementation turns out to be.
- Only partially platform independent. The web service is platform independent, however the application on the smartphone is not.
  * Low re-use, only parts of the existing system can be re-used.
  * High amount of work required.

### 5.1.4 Rebuild 2

Access the business system through a new web service using an Android application that containing a webview.

- Strödata has complete control over both the application and the web service and their code.
- The GUI of the application will be adapted for smaller screens.
- Good possibilities for further development.
- Limited functionality of the application (limited to the original idea of work reporting). Depending on how difficult and time-consuming the implementation turns out to be.
- Only partially platform independent. The web service is platform independent, however the application on the smartphone is not (in this suggestion the smartphone application is smaller and simpler than in the previous one, therefore it is easier to develop equivalent applications for other smartphones).
- Generally not good practice to create an application which only shows a web page.
  * Low re-use, only parts of the existing system can be re-used.
  * High amount of work required.

### 5.1.5 Rebuild 3

Access the business system through a new web application using the smartphone's browser.

- Platform independent, can be accessed through any browser on any smartphone (assuming they have support for SSL and certificates).
- The GUI of the application will be adapted for smaller screens.
- Good possibilities for further development.
- Limited functionality of the application (limited to the original idea of work reporting). Depends on how difficult and time-consuming the implementation turns out to be.
  * Low re-use, only parts of the existing system can be re-used.
  * High amount of work required.

### 5.2 New application use case

In this section, a use case for the application that is to be implemented as part of this project thesis is presented. The use case is based on the original use case that is presented in section 2. The new use case will show some of the differences between the original use case, and a use case with smartphone access to the work report creation part of the business system implemented.
Peter is employed by Strödata, he has just finished his current assignment and he wonders if he could fit in another client assignment before the day is over? Of course, he still needs to create a work report for the finished assignment and when that is done he needs to find a new assignment. Peter fishes his smartphone out of his pocket and starts the web-browser. He navigates to Strödata’s new web-application and logs in. As the company policies state, he has not saved his user credentials on the smartphone so it’s a little more work than it could be. But at least it is a bit more secure. Then he navigates to the work report creation page. Once the page is loaded, Peter fills out the form and saves the work report. I’ll approve it when I stop by the office. Now if I only could access the available assignment through the smartphone as well, Peter thinks. I suppose I can call the office and ask them to select a new assignment for me, that way I don’t need to drive there and then out to the client, I can go straight to the client. That would shorten the travel time.

5.3 Development
From the suggested solutions that were presented in the previous section (5.1), the “Rebuild 3” suggestion was selected by the client. The concept of the solution is to implement a new web
application for work reporting as a proof-of-concept of smartphone access as part of the business
system. The new web application will be adapted to work on smartphone screens as well as computer
screens. The purpose of the new web application is to make work reporting fast and simple while the
employee still has details fresh in memory. To minimize the amount of work required on the
smartphone, the work reports that are submitted through this new web application will not be set to
the status “ready to be billed”. This means that only certain fields require input and that the report is
not completed, therefore the company’s customer cannot be billed for the work yet. For example:
writing a description of the work that has been performed is not a task best suited to be performed on
a smartphone. This field can be left empty and filled in later, when the employee has returned to the
office and has access to the entire business system. There he/she can access the work report and
complete it. Even if the user has filled in all of the input fields, the report still needs to be confirmed in
the original business system since there are follow-up tasks to the work reporting activity that are not
within the scope of the new web application and therefore will not be implemented.

The new web application will more or less be a form which the employee fills out with the work report,
the same as for the original web application. It will require the user to log in using the same credentials
as in the original system. All traffic will be encrypted using SSL, same as in the original system. The
differences between the form for work reports in the original and new web application will be
described later in this section.

The new web application will be an ASP.NET MVC3 site that uses JavaScript, jQuery and Ajax-JSON.
The reasons that ASP.NET was chosen for the development of this proof-of-concept application is that
ASP.NET is not only a free framework, it is also very well known and much used framework for
implementing web sites. ASP.NET has different approaches to implementing web sites, there is the
web page approach, the web forms approach and the MVC approach. For this project thesis and this
proof-of-concept application I chose the MVC approach. To be more specific, the MVC3 design pattern.
At the time of this choice MVC3 was newly released (at the time of writing MVC4 has been released as
well) which was the reason I chose the MVC3 release rather than the older MVC2. The MVC design
pattern is explained below.

Since the web application uses the MVC design pattern there will be several models, views and
controllers [6]. The models represent each of the tables in the database. The views display the user-
interface to the user. The controllers handles the user interaction, they work with the model, and select
a view that displays the appropriate user interface.

Also in the model is a class to use with a form in the work report view. Since the information needed
from the user to create a work report includes different information than what is stored in the work
report table in the database, an additional class that has the needed parameters will be used, a form-
class so to speak. Some of the data that is stored in a work report post in the database is collected
from other tables in the database, other data is auto-generated. There are also other tables than the
work report-table that are affected when a work report is created and the required information for
these posts need to be collected from the user as well. An object of this form-class is used in the
controller action method to receive the user input from the form. In the controller action method the
work report entry for the work report table etc. are created and inserted into the database.
After discussions with other web developers regarding the dynamic content of the proof-of-concept application I decided to use JavaScript, jQuery and Ajax-JSON to deal with the changeable content of the application. By using JavaScript on parts of the application it gives an immediate change of the content, rather than reloading the entire page only to change a subsection of the content. This is due to the fact that the JavaScript is executed on the client rather than the server. The reasons behind using jQuery and Ajax-JSON are solely based on the recommendations of other web developers I had discussions with, among them the developer of the current business system. jQuery was used to manipulate the content of the database using JSON-objects to handle the output to and input from the jQuery commands.

In regards to smartphone access to the business system and the risks involved, there are a number of actions that are taken when implementing this proof-of-concept application. To start with, the technology that is used in this proof-of-concept is much newer than the technology used to implement the current application. Rather unsurprising since the current application was implemented in 2004, there have been significant changes to the technology that is available since that time. That being said, the methods and the technology that was chosen for the implementation of the proof-of-concept are by no means new and experimental. They are tried and true, which is a large reason why they were selected.

Looking at the input, it was decided to make as little input as possible required to create a first draft of a work report. For the reasons that it should be fast and simple to create a work report before the details of the assignment are forgotten. As well as to minimize the amount of information that must be entered through the smartphone. A smartphone is not well suited to write long texts, such as long descriptions, but writing short descriptions or short input is done simply enough. The implementation also includes input validation. Most input fields when creating a work report has some restrictions on the input that is allowed. For example, the amount of time spent on an assignment must be entered into the input field in specific way to match the representation in the database, more on these restrictions below. The input validation is performed using validator controls. Validator controls are a part of ASP.NET and they can use regular expressions to validate the information that is entered into input fields, on the client-side. This means that the validation is not performed on the server-side which gives much quicker feedback to the user since the information does not need to travel to and from the server in order to be validated.

In regards to the vulnerability of saved user credentials, the log in page in the proof-of-concept application does not provide the option to remember the user credentials. The browser is instructed, through HTML, to not allow the user the option of saving their credentials. A small precaution that is taken when the user enters a username and password that do not match (either because the username is incorrect or because the password is incorrect) is the error message that is presented. The error message does not state which of the input fields is incorrect, in order to provide a possible attacker with as little information as possible. Section 4.1 explores the risks concerning smartphone access to Strödata’s business system further.

The new web application will have some differences in the user interface compared to the original web application, below is a list of differences.

---

73
• There is no longer a checkbox to indicate if the work report is a part of a project or not. Instead there is a drop-down list with the available projects for the selected company. The first element in the drop-down list is empty and should be selected if the report is part of a project.
• The date input has been changed from a calendar to a text input box where the date should be written on the format: four digit year, two digit month and two digit day (YYYYMMDD).
• Reports for companies and projects with constant prices will have two input fields, one is a drop-down list with preset prices and one is a text input box for a custom price. The first element in the drop-down list is empty and should be selected in order to use the custom price.
• Reports for companies and projects with variable prices (prices per kilometre and hour) will have four text input boxes (number of kilometres, price per kilometre, time and price per hour). In the input text boxes for the prices the default prices will be shown by default. These should be changed if the default price should not be used. The time input should be written on the format: two digit hour and two digit minute (HHMM).
• Every work report has a “Veckorapportsunderlag för framkörning” input field, in which there are two text input boxes. The first is for the number of kilometres. The second is for time, which should be filled in on the format: two digit hour and two digit minute (HHMM). There is no longer a confirmation-checkbox in the “Veckorapportsunderlag för framkörning” field.
• Invalid input will result in error messages below the corresponding input field. The error messages will inform the user that the input is invalid and why.

The list above gives an idea about how to fill out the work report form, below follows more detailed instructions.

To minimize the amount of work that needs to be performed to create a work report through the smartphone there are very few required input-fields. They are: the name of Strödata’s customer company and the date. If a company is not selected no work report can be created, the same reasoning applies to the date.

The webpage is divided into sections, the sections are displayed depending on which company and project are selected. Some of the sections should be filled in no matter which combination of company and project is selected, these sections are displayed at all times. The permanent sections contain:

• The customer company name, the contact person at the company and the project.
• The work description (date and description).
• The “Veckorapportsunderlag för framkörning” (number of kilometres travelled to the client and the time spent working on the assignment).

There is also a project description section that is only shown when a project is selected. Depending on if the selected customer company and/or project has a fixed cost for Strödata to perform a task or not, one of the two remaining sections are displayed. The first section contains a list of preset prices and a custom price field. The other contains input-fields for the following variables: number of kilometres to travel to the customer, the price per kilometre, the time spent on the customers’ assignment and the price per hour. See Error! Reference source not found. for mockups of the form.
Due to the data-types used to store the work reports in the database, most of the input needs to be formatted in a specific manner. Table 41 shows the constraints for each input field (excluding the drop-down-lists).

<table>
<thead>
<tr>
<th>Input field</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arbetsbeskrivning (Work description)</td>
<td></td>
</tr>
<tr>
<td>Datum (Date)</td>
<td>• Mandatory. • Length of the input must be eight characters. • Input may only be numbers. • Input must be formatted as YYYYMMDD (four digit year, two digit month and two digit day).</td>
</tr>
<tr>
<td>Beskrivning (Description of the job)</td>
<td>None.</td>
</tr>
<tr>
<td>Företag/projekt med fast pris (Companies/projects with set price)</td>
<td></td>
</tr>
<tr>
<td>Anpassat pris (Custom price)</td>
<td>• Input must be digits, “,” or “.”.</td>
</tr>
<tr>
<td>Företag/projekt utan fast pris (Companies/projects without set price)</td>
<td></td>
</tr>
<tr>
<td>Antal kilometer (Number of kilometres)</td>
<td>• Input must be digits.</td>
</tr>
<tr>
<td>Pris per kilometre (Price per kilometre)</td>
<td>• Input must be digits, “,” or “.”.</td>
</tr>
<tr>
<td>Tid (Time)</td>
<td>• Input must only be numbers. • Length of the input must be four characters. • Input must be formatted as HHMM (two digit hour and two digit minute).</td>
</tr>
<tr>
<td>Pris per timme (Price per hour)</td>
<td>• Input must be digits, “,” or “.”.</td>
</tr>
<tr>
<td>Veckorapportsunderlag för framkörning (Base for weekly report)</td>
<td></td>
</tr>
<tr>
<td>Antal kilometer (Number of kilometres)</td>
<td>• Input must be digits.</td>
</tr>
<tr>
<td>Tid (Time)</td>
<td>• Input may only be numbers. • Length of the input must be four characters. • Input must be formatted as HHMM (two digit hour and two digit minute).</td>
</tr>
</tbody>
</table>

Table 41 Input constraints for the work report form

If the constraints are not met, a notification text is shown below the corresponding input field.

When the input is valid the user may create the report by clicking the “Skapa rapport”-button at the bottom of the form. If the report is properly inserted into the database the user is redirected to the “Done”-page to show this. The “Done”-page simply states that the work report has been created. If the report fails to be inserted into the database in spite of the input validation, the user is redirected back to an empty work report form as a fallback.
5.4 Demonstration

This section of the report describes how the demonstration of the proof-of-concept application was performed, as well as the feedback from the representatives from Strödata after the demonstration.

The demonstration of the proof-of-concept application was performed during a meeting with the CEO, the CTO and I, the developer. The demonstration contained three steps. The first step was the demonstration of the proof-of-concept application on a smartphone. The second step was the demonstration of the proof-of-concept application on a laptop. The third, and final, demonstration step was performed on the current business system, on a laptop. The intention of the third step was to show that the first and second demonstrations inserted correct work reports into the database.

The demonstration of the proof-of-concept application on a smartphone was performed according to the following general steps:

1. Access webpage
2. Log in
3. Complete the work report form
4. Submit work report
5. Log out

Looking at the above mentioned steps of the demonstration, one can realize that they represent the sunshine scenario. A scenario that is as simple as it can be and where every action is correct. This of course does not reflect the real life scenarios where the proof-of-concept application could be in use. In the sunshine scenario there are for example no typos. The proof-of-concept application must be able to handle incorrect input for those times that are not contained in the sunshine scenario. Therefore the demonstration must contain non-sunshine scenarios as well, or verification that the application works as intended cannot be accepted. For this reason, each of the above mentioned steps of the demonstration contains more scenarios, which are described below.

Step 1 is very straight forward, any deviation from the sunshine scenario here is not a part of the demonstration. The focus of the demonstration is the proof-of-concept application, not the URL of it or how to reach it.

Demonstrating step 2 is also rather straight forward. Attempting to log in with a correct username and an incorrect password (and vice-versa), yields an error message stating that either the username or the password is incorrect. Not which of the two is incorrect, stating which attribute is incorrect would give too much information to anyone trying to gain unauthorized access to the system.

Step 3 is more extensive. There are several input-fields which require a specific format on the input, each of these needs to be demonstrated. To make the demonstration as complete as possible without taking too much time, most of these input verifications can be performed in groups. Several input-fields depend on the choice made of previous input fields. For example, different customers have different contracts with Strödata, some have a set cost for work while others pay an hourly rate. The input requirements for the different fields are explained in the previous section of the report (section 5.3), all these are demonstrated.

Step 4 is very straight forward as well. When the work report is submitted by pressing the “Skapa rapport”-button at the bottom of the form the user is redirected to the “Done”-page. Unless the input
values are rejected by the database in spite of the input validation that is in place, in which case, the user is redirected back to an empty work report form. Both alternatives are demonstrated.

Step 5 is straightforward as well. By clicking the “Logga ut”-button, the user is logged out of the system and directed back to the log in page. Once logged out, the user can no longer access any other part of the application than the log in page.

The demonstration steps presented above are performed both on a smartphone and a laptop to show that the proof-of-concept application works on both types of devices, and that the proof-of-concept application contains all the elements that are needed to complete the task of creating work reports.

To further demonstrate that the proof-of-concept application works as intended, and that the correct data is inserted into the database, one more demonstration is performed. By using the current system, the latest work reports that have been created are shown. These work reports should of course correspond to the reports created using the proof-of-concept application in the previous demonstrations.

The demonstration was performed successfully with the proof-of-concept application performing well. The application passed the tests/steps mentioned above with flying colours. All the different types of work reports were successfully created using both smartphone and laptop. All input fields showed the appropriate error messages for invalid input, and no malformed input was allowed past the input validation. Both representatives of Strödata shared the opinion that the proof-of-concept application indeed did prove the concept of smartphone access to the system. They also agreed that smartphone access to the business system should be enabled in the, not too distant, future.

However, after some discussion between the Strödata representatives and myself, it was decided that the proof-of-concept application should not be deployed to the active system. This was largely due to the fact that during this project thesis Strödata decided to update their business system to a new web based business system that covered the entirety of Strödata’s needs. A decision which was in part due to the findings from the risk analysis that was performed during this project. The new system they have in mind is also prepared for smartphone access already. So, it was decided that a requirement on the new system would be the possibility to either activate smartphone access or to have it out-of-the-box. With this as a base, it was decided that the proof-of-concept application should not be deployed to the active system in the interim time before the new business system is fully deployed.
6 Discussion and conclusions

The motivation behind this thesis project was to implement access to Strödata’s web based business system through a smartphone, or rather, access to a part of the system. Since access to the company’s business system means access to the company’s database and all the information in it, the security of that information is a concern. Therefore the risks to the system caused by access through smartphones needed to be analyzed. Due to that, it was necessary to perform a risk analysis on the original system as well. The risk analysis of the original system is needed to see the current state of the risks posed to the system and to have a base for the analysis of the smartphone access. Part of the risk analysis of the original system is to identify treatments for the risks that have been identified. The idea that smartphone access might be among these treatments was conceived while discussing the risks to the original system. Among the risks is the “Forgotten details”-threat scenario, which for example means that details about performed assignments for a customer are forgotten, such as the amount of time spent on the task. These deviations might not be very large on their own, but when there are enough of them they build up and may cause a loss in income for Strödata. This is part of where the idea about smartphone access as a treatment came from. Before the idea that smartphone access could be a possible treatment, it was more a matter of convenience and another step towards making the business system as mobile as it could be. As the risk analysis has shown in the previous sections of this report (section 3 and especially 3.7) smartphone access is a possible treatment.

How should the proof-of-concept of smartphone access be implemented? And in extension, full access through smartphones? At the very start of this thesis project the idea for smartphone access was an implementation of a smartphone application for the Android operating system. But through discussion with the developer of the original business system and representatives from Strödata the possibility to make the access possible from all smartphones, independently of operating system, was decided to be a strong option. Section 5.1 contains a list of the suggestions for the smartphone access that were identified during these discussions. The solution that was eventually selected was “Rebuild 3”, which is the development of a new web application that can be accessed from all smartphones, as well as computers, independently of their operating system. The new web application that has been developed is an ASP.NET MVC3 site that uses JavaScript, jQuery and Ajax-JSON. The proof-of-concept implements access to the creation of work reports.

So, if the purpose of the thesis project was to analyze how smartphones access to the business system affects the risks posed to the system and to implement a web application with limited functionality for that access. Was the purpose achieved? Yes, I believe it was. The risk analysis showed that smartphone access can lower certain risks to the system. While it also creates new risks to the system they are not large enough to outweigh the benefits of such an access. The proof-of-concept web application for reporting work to the system was implemented and it is functional. It also fulfils the security requirements which were quite important. There are of course improvements to the web application that could be made. For example, the user interface is the same for large screen as it is for small (smartphone) screens. It is quite possible to implement one user interface for smartphones and one for computers. It is possible to detect if the visiting user is using a smartphone or a computer and you can redirect the user appropriately to an interface that is even better suited for smartphones. There are endless possibilities for features when using a smartphone rather than a computer. Using the smartphones GPS is just one idea. You could for example implement a start-finished time feature for the system. When the employee starts to move to a client from the office he/she activates the feature.
This starts a time-counter and a distance-counter (which uses GPS to find the smartphones location). When the employee is finished with the assignment for the client he/she stops the feature and is presented with a work report form with time spent on the task as well as distance travelled already populating the form.

Other than the fact that smartphone access may be a treatment for a lack of availability of the system, what did the risk analysis show? It showed among other things that there are significant risks to the system that require evaluation. Each of the threat categories provide some risks that need to be treated. The risks that need to be treated all affect the “Financial information”-asset, this is probably not very surprising since the financial information directly affects the company’s profits and losses. If invoices cannot be sent to the customers, the customers will not pay. The result of this is rather obvious. The analysis also showed that employees can cause large amounts of damage to the company, be it through carelessness, lack of knowledge or malice. Perhaps not a very surprising result, since it is well known that “insider-threats” are among the greatest threats to any system. The insider has a familiarity with the system that an outside threat probably does not have. The amount of things that an employee can do to cause harm to the information in the database ranges from deliberately changing data to accessing data and then leaving it on the screen for all to see through carelessness.

When comparing the threat diagrams for the different kinds of threats (human intentional, human unintentional and non-human) the human unintentional is by far the most complex. Many of the vulnerabilities interconnect and many of the threat scenarios lead to the same unwanted incidents (this is not surprising considering the way the unwanted incidents were divided). Another thing the analysis showed is that there are several risks that cannot be treated successfully with the treatments that were identified in the risk treatment step (section 3.7). The treatments do not quite reduce the risks enough to be acceptable, but they are moved closer to acceptable values. Perhaps close enough to lead to a re-evaluation of when the risks are acceptable. The treatments that were identified did show a rather large reduction in calculated losses if they are implemented. 6 975 280 SEK, at least, is not pocket change even if that amount is over a ten year period (697 528 SEK per year).

The risk analysis that is part of this thesis project is specific for Strödata, their system and their situation. Attempts were made to make the analysis somewhat general. For example, the hacker-threat is present for all businesses. The level of the threat would be similar when comparing Strödata to any other IT company of a similar size and in a similar situation. Considering the consequences the unwanted incidents may have, they will most likely vary a great deal between Strödata and other similar companies. The assets could be valued differently by another company, perhaps they would consider their “Customer information”-asset to be more business critical than their “Financial information”-asset. This other, similar, company may not even have their financial information in the same system with other information, such as customer information, the way Strödata has their system set up. Therefore it would not be applicable to the risk analysis. Both the threats and the vulnerabilities that have been identified in this analysis are intentionally rather general. They are broad enough to be applicable to any business with a web-based business system connected to the company database.

Focusing first on the threats, the human threats of hackers, malicious employees and ordinary employees, are all threats that are common for most business systems. It does not matter what size the company is or what systems they use. The hacker-threat is always present to some extent, more or less depending on the business type. As for the employees, they always pose a risk to the business, whether it is with intent or not. An unknowing employee can cause a lot of damage to a company, for
example by giving company confidential information to a “friend”, as part of an everyday conversation. The malicious employee damages the company intentionally, whether it is by taking information to a competitor or erasing the company database out of spite after being laid off. The non-human threats that have been identified in this risk analysis are also rather general and applicable to any web-based system of any kind. However, there are of course other non-human threats that should be taken into account when analysing a system. Some examples are environmental threats such as floods, hurricanes or something as simple as the plumbing in the building. A water pipe that starts to leak in the wrong place could be devastating. Here is where the analysis gets more specific to Strödata’s situation. Strödata’s buildings are in good shape and there are no violent environmental phenomenon’s that could cause unwanted incidents in the regions where the offices are located. Therefore these types of threats were dismissed and the focus of the analysis was placed on the technical threats. The choice was made to categorize these threats in very general categories regarding the system itself and the communication with the system. These threats can of course be taken apart and defined as numerous more specific threats. That was however not how the representatives of Strödata viewed them. Therefore the larger categories were chosen.

Looking at the vulnerabilities, these are also intentionally rather general, and can be applied to other businesses and systems of the same type. For example, such vulnerabilities as “Lack of training” or “Insufficient policies” affect any businesses and any system. Employees need to be educated in how to use the systems and they also need to know what they are allowed to do, both, with the systems and with the information the systems may contain. There are however one vulnerability that stands out, “Insufficient availability of the business system”. This vulnerability is one of the reasons this project thesis was created. The idea that the business system should be as accessible by the employees as possible is a focus point for Strödata. With the emergence of smartphones there is a new way to access the business system, however today that is not possible. This is what creates the vulnerability. Other businesses may not place as much weight on the availability of the business system as Strödata does. They may be satisfied with the fact that the business system is available through computers and do not see the need to access the business system through smartphones as a problem.

Moving on to the risk scenarios and unwanted incidents, these are also intentionally rather general and can be applied to any business with a web-based business system connected to the company’s database. They are also based on the previous entities (threats, vulnerabilities and in the unwanted incidents cases, the risk scenarios) that are also described as rather general.

The assets that have been identified in this project thesis are very specific to Strödata. They represent the entities in the business system that Strödata wants to keep safe and confidential. They can of course be applicable to other systems and businesses but as they are defined specifically for how the representatives from Strödata view their assets, they would be less specific if applied without thought to other systems. The assets in a risk analysis are one thing that truly needs to be defined specifically for that client. Although a prepared set of general assets may be of great help when defining the clients’ assets. For example an asset labelled “Customer information” may very well have different meanings in different companies and systems. It could mean anything from the contact information for the customer to their date of birth, their previous purchases and their credit-card information. But most companies do have some sort of customer information stored. It is important to take that into consideration when defining the assets and later when the consequences of incidents are defined and calculated.
What further sets companies apart in a risk analysis is how they define the likelihood scale and the consequence scales for the assets. For example, one company may have rigorous policies (preferably official policies, but unofficial spoken or unspoken rules also have an impact) in place regarding the use of their business system, and therefore the likelihood that an unwanted incident that is based on the vulnerability “Insufficient policies” should occur is rather low. Compare this to a company that has no policies in place regarding the use of their business system, the likelihood of an unwanted incident based on the same vulnerability is much higher than for the company with rigorous policies. The same reasoning applies to the consequences of unwanted incidents. One company may store much more (sensitive) information in the database that is connected to their business system that all employees use every day, than any of their competitors. Therefore the consequences for an unwanted incident that affects the database information would have harsher for this company than it would have for its competitors.

How can the results of this thesis project be used? The risk analysis can be used to reduce the risks to Strödata’s business system and thereby reduce the losses they cause. The risk analysis has shown that smartphone access to the system is not a bad idea. The new web application can be used to report work as it is, but is can also be further developed. In its current state it only supports work reporting, the remaining features of the business system can also be implemented in the new web application. Since the new web application is accessible both through smartphone and computer it could eventually replace the current business system. This would also be one of the treatments that have been identified, updating the WebApp. The fact that smartphones have additional features, such as GPS, also opens up some interesting features, such as the start-finished feature mentioned above.

In section 1 of this report, a number of questions were posed. These questions have been answered throughout the report, but to give a short and clear overview of the questions and their answers they are presented below.

- **What new risks, if any, would smartphone access to Strödata’s business system cause?**
  - Introducing smartphone access to the business system will add new risks to the system. The first new risk to the system would be a thief that steals a smartphone from an employee and thereby gains access to the information in the database. The second new risk would be a hacker, who somehow installs spyware on an employee’s smartphone and thereby gains access to whatever information the employee accesses using the infected smartphone. See section 4.1 for more details.

- **Could the smartphone access decrease or even completely remove any existing risks posed to Strödata’s business system?**
  - Smartphone access to the business system would increase the availability of the business system to near 100% (considering the telephone network providers data traffic coverage in the area where Strödata operates). The availability of the business system would be close enough to complete that the vulnerability “Insufficient availability of the business system” is eliminated. See section 4.1 for more details.

- **Is it possible to implement access to Strödata’s business system from computers, smartphones and anything in between the two?**
  - It is possible, in a number of ways. Examples of how this can be achieved are: implementing a smartphone/tablet application which communicates with the company database, adapting the existing web application for use on smaller screens
or implementing a new web application, which communicates with the company database and is adapted for smaller screens. See section 5.1 for more details on possible solutions.

- What would be a satisfying way to implement access to Strödata’s business system for anything between computers and smartphones?
  - As mentioned above, there are multiple possible solutions to choose from. The solutions where a new smartphone application was to be implemented were discarded on the grounds that not all employees use the same operating system on their smartphones. To grant access to all employees several smartphone applications would need to be implemented. The solutions where the existing web application would be adapted for smaller screen were also discarded. The solution where a new web application should be implemented was selected. The new web application would be implemented using ASP.NET with JavaScript, jQuery and Ajax-JSON. See section 5.3 for more details on the selected solution and the implementation.
References


Appendix A Mockup of new web application
This appendix contains the mockup images for the newly developed proof-of-concept web application.

Figure A.1 Desktop view of mockup for customer without project selected and without fixed price
## Strödata

### Kund information

**Kund**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

**Kontaktperson**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

**Projekt**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

### Arbetsbeskrivning

**Datum**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

**Beskrivning**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### Företag/projekt utan fast pris

**Antal kilometer**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

**Pris per km**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

**Tid**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

**Pris per timme**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### Veckorapportsunderlag för framkörning

**Antal kilometer**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

**Tid**

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

[Skapa rapport](#)

*Figure A.2 Smartphone view of mockup for customer without project selected and without fixed price*
**Strödata**

**Kund information**
- Kund
- Kontaktperson
- Projekt

**Arbetsbeskrivning**
- Datum
- Beskrivning

**Projekt**
- Beskrivning

**Företag/projekt med fast pris**
- Fast pris
- Anpassat pris

**Veckoraportsunderlag för framkörning**
- Antal
- Tid

[Skapa rapport]

*Figure A.3 Desktop view of mockup for customer with project selected and with fixed price*
Figure A.4 Smartphone view of mockup for customer with project selected and with fixed price
Appendix B Copyright

På svenska

Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extra-ordinära omständigheter uppstår.

Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art.

Upphovsmannens ideella rätt innefattar rätt att bli nämnt som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se förlagets hemsida http://www.ep.liu.se/

In English

The publishers will keep this document online on the Internet - or its possible replacement - for a considerable time from the date of publication barring exceptional circumstances.

The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: http://www.ep.liu.se/

© Anton Nilsson