MASTER'S THESIS

Mitigating Data Leakage by Enforcing the Information System Security Policy

Rune Millerjord
Oscar Sundström

2015

Master (120 credits)
Master of Science in Information Security

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

LULEÅ
UNIVERSITY
OF TECHNOLOGY

MITIGATING DATA LEAKAGE BY ENFORCING THE INFORMATION SYSTEM SECURITY POLICY

Rune Millerjord

Oscar Sundström

Master Program
Master of Science in Information Security

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering

COPYRIGHT

Contact Information:

Project Member(s):

Rune Millerjord
E-mail: runmil-3@student.ltu.se

Oscar Sundström
E-mail: oscsun-9@student.ltu.se

University Advisor:
Devinder Thapa
E-Mail: devinder.thapa@ltu.se

LULEÅ UNIVERSITY OF TECHNOLOGY
Department of Computer & Electrical Engineering
Division of Computer and System Science
SE-971 87 Luleå
SWEDEN

Abstract

Data which leaves the organization perimeter leaves the organization's control as well. This means that once the data is revealed there is no possibility to undo it, no logging, no access rights, no remote deletion etc. This is something which most organizations show an increasing concern of over the last couple of years. Information System Security Policy (ISSP) is the main tool used today to limit what data is leaving the organization. For the ISSP to be efficient it must be kept up-to-date, every individual needs to know and follow it and that security controls are implemented to control compliance with the policies. Another tool to control what data is leaving the organization is to implement Data leakage Prevention (DLP) which is a technical solution to enforcing the ISSP.

In this research we looked into what ISSP breaches can be mitigated by implementing data leakage prevention solutions which enforces the ISSP to limit what data that can leave the organization’s perimeter. We therefore utilized a conceptual framework which combines the theory of planned behavior with SETA to determine whether the data leakage is intentional or unintentional based on the individual's intent and compliance with the ISSP.

Two organizations decided to participate in this research which we interviewed. The questions were in regards to how they handle data leakages, how their ISSP looks like and what data is confidential. A DLP was also implemented in the organization's network to scan and log the outgoing data based on keywords we defined from the policies and common practice. Their ISSP was also copied and later analyzed together with the network scan and interview to get the result which should answer the research question.

The results of our findings was that on average there was more than three data leakage

incidents per day. It seems like all of these were due to people not following procedures or policies. On the other hand it did not seem like there was any malicious behaviour behind the incidents. Another finding was that the policies was not as good as they could have been.

The conclusion of this research is that unintentional data leakage can be prevented by having a good security culture with a high level of security awareness. But you can’t prevent what you don’t know of. You need the visibility on what type of data is leaving the company premises, and a DLP solution will help you with that. Having a data leakage prevention system will be the technical replacement of a good security culture, but it might even limit persons with malicious intentions.

Acknowledgement

A lot of people were involved in shaping this Master thesis into what it is. Unfortunately we cannot honor them all, but it is our privilege to recognize those who deserve a special note.

To Luleå University of Technology would we like to express our greatest gratitude in allowing us to study Information security and the opportunity to work on this Master thesis with them.

To our professors and supervisors would we like to present our sincerest “thank you” for their guidance, support and help in completing this Master thesis.

To the participated organizations would we like to express our gratitude for their participation, which without wouldn’t make this thesis into what it is.

To Checkpoint Sweden we present our deepest thanks for whom lent us a firewall with capabilities to perform necessary traffic analysis with data leakage prevention features.

Contents

Chapter I

1 Introduction

More and more organization are expressing increasing concern towards data leakage in the recent years (Ahmad et al, 2013; Blasco et al, 2012; Colwill, 2009; Walker, 2008). Organizations today are relying on information systems to produce or manage the products which are their main source of income, this makes it of utter importance to make the data stay within the company perimeters.

Every year the Ponemon institute publishes a report on data leakage. During 2013 there were 277 reported incidents with a total of 23,647 compromised records of data, which on an average meant the loss of $136 dollars per record (Ponemon Institute, 2013). This resulted in the total loss of $3,215,992 dollars during 2013 alone because of data leakages. In 2007 the UK Government's Revenue and Customs Department (HMRC) fell victim to data leakage where 25 million peoples had their personal information compromised during a single incident. The result of data leakages is therefore not limited to only economic losses.

Other common results of data leakages is the loss of competitiveness and economical fees (Ahmad et al, 2013; Blasco et al, 2012). Organizations who are victims of data leakage can have a very difficult situation in competing against other organizations in the same marked since their customer might not trust them anymore. The organization might even have to pay a settlement to their customers which data was compromised, something the organization might never come back from.

Most organizations spend several thousands of hours and a lot of money in developing policies, binding agreements, security controls and more in orders to secure their assets as well as the organization itself from threats (Brendan, 2014). Organizations rely on their security to keep theirs and their customers confidential data secure from unauthorized parties. Most organizations are concerned of losing the controls over their confidential data once the data has left the organization's perimeter (Blasco et al, 2012; Colwill, 2009). Once the confidential data has been brought out of the company is impossible to control the confidentiality, integrity and availability of the data. This means that once confidential data has been disclosed by leaving the organization it is impossible to prevent who gets a hold of the data.

1.1 Research objective

Since the issue of data leakage has become an increasing concern for most organizations, the objective of our Master Thesis study is to analyze *how organizations are experiencing data leakages despite policies being implemented* as a motive on solving the data leakage problem. This is a very important topic for organizations and their capability to prevent confidential data from leaving the organization. This is achieved by doing a detailed case study on information system security policy and data leakages in organizations.

1.2 Definition of data leakage

Data leakage is the phenomena when confidential data is being disclosed unintentional or intentional to unauthorized parties without the permission of the author. Data leakage can in turn lead to information and knowledge leakage when the data is put into context. Hence, encrypted information is a form of data and can therefore be considered as data leakage as well.

1.3 Organization Details

Company 1 is a Swedish municipality. There are approximately 1800 employees in the municipality, where IT is centralized into the main datacenter. They are performing normal municipality services like running elementary schools, social services, care facilities for the elderly and technical services like water cleansing and waste recycling.

The second company that participated is a software development company with branch offices around northern Europe. In total the company has approximately 400 employees, most of them working in the headquarter in Sweden. They are creating their own software that they sell to customers. They also give remote support to their customers through secured access to the servers at customer sites.

1.4 Problem Definition

Earlier studies shows that most organizations tends to develop and implement security solution which mostly secure their confidential data against external threats but neglect the internal threats (Brendan, 2014; Colwill, 2009; McCue, 2008; Adams & Sasse, 1999). This causes an imbalance in the organization's security architecture where data is secure from traditional threats which try to force their way through the security mechanism from outside of the organization. These security mechanism doesn't appear to stop confidential data from being brought out of the organization, which is a great concern for most organizations.

Data leakage is not limited to occur through malicious acts, data leakage can also occur through accidents (Annansingh, 2005; Blasco et al, 2012; Colwill, 2008) and it is not uncommon that unintentional data leakage are more severe compared to intentional data leakage (CSO, 2010; Blasco et al, 2012; Colwill 2008) . Even though data leakage itself is bad for the organization, unintentional data leakage has the power to cause greater harm to the organization because the source of the data leakage might not be found and could occur several times.

A study by BERR (2008) reveals that most organizations don't scan their outgoing communication, encrypt their hard drives or preventing flash-memory from taking confidential data out of the organization. This is a huge issue were simple email exchange with friends could contain confidential data which can result in data leakages. According to earlier studies, most types of electronic communication unmonitored and uncontrollable (Blasco et al, 2012; Colwill, 2009). Once an e-mail containing confidential data are sent out of the organization, the organization can no longer control the disclosure of the data.

Modern organizations try to encourage the work practices through teamwork and shared responsibility and are relying on trust and information sharing. Organizations want a more efficient workplace by implementing teamwork and shared responsibilities by relying on trust and information sharing (Ahmad et al, 2014; Adams & Sasse, 1999). It's not uncommon for organizations to just trust the users within the organization's perimeter with not enforcing their policy on the users, which raises a few data leakage concerns. Is trusting the users the only viable option in preventing data leakage?

1.5 Thesis Outline

Chapter II is a literature review on previous research regarding data leakage, data leakage prevention, ISSP, insider threat and compliance.

Chapter III provides an overview on earlier studies using the same theoretical framework, why and how we have used it in our research.

Chapter IV explains the details of research methodology where we have described the details of the research type, ways of data collection and analysis.

Chapter V provides the data which was collected from the different sources.

Chapter VI contains the analysis of the collected data.

Chapter VII provides the conclusion of the research and future research in the field of data leakage.

Chapter VIII contains the references.

Chapter IX contains the appendices.

1.6 Research Questions

How can enforcement of Information Systems Security Policies mitigate unintentional data leakage?

1.7 Thesis Limitation

Although the research was carefully planned and performed, we can’t ignore some of the limitations that arise. First, because of the security concern which this research possesses against the organizations, this research was therefore conducted with a smaller amount of participants which didn’t mind the security concern. Therefore, to generalize the result for larger groups, the study should have involved more participants in different sections. Second, because of economic reason, this research was performed with participating organizations established within Sweden. This research was therefore performed on a smaller group which we could travel to in order to collect the data necessary to perform this research.

Chapter II

2. Literature review on previous research

To find the gap in the research field of ISSP enforcement and data leakage prevention we have to go through what other researchers has done prior to this study. The material available is quite extensive on both subjects, but the impact of not enforcing the ISSP hasn't been found during our literature review.

2.1 Data leakage

Data leakage is defined as unauthorized disclosure of sensitive information to unauthorized parties through accidental or deliberate acts (Shabtai's et al, 2012; Blasco et al, 2012; Annansingh, 2005). These studies define data, information and knowledge leakage in a very similar way. Bellinger et al (2004) states that data is raw, and doesn't have any significant meaning by itself. Once the data has been given a meaning through relations with other data it changes state into information. Data which is intended to be useful and appropriately collected becomes knowledge. By reviewing these studies, one can come to the conclusion that data influences information and knowledge and that data leakage can also result in information and knowledge leakage. Based on this review, is data leakages actually a problem since data is defined as raw and doesn't have any significant meaning? Bellinger et al (2004) states that what someone sees as data someone else sees as information. If you leak a larger amount of data, someone can put that together to information.

Colwill (2009) argues that insiders exist within most enterprises today even though the enterprise itself might not know of them, which is a growing concern. A recent survey by the

RSA/IDC found that most chief security officers (CSOs) were more worried about external threats and that 82% of the respondent didn't even know where the company's insider risk were located. The survey also revealed that 5830 malware attacks originated from within the enterprise and 5794 incidents where insiders abusing their access control rights and that 19% of the attacks were deliberate (Grant, 2009). Ponemon Institute publishes annually reports on data leakage and in 2013 there were 277 cases of data leakage with an average of 23647 records of data being leaked. On average the value of each record was $136 dollars (Ponemon Institute, 2013). By reviewing these studies, one can find that insider threats do exist within enterprises right now, but the security management choose to turn a blind eye to it despite that a single attack compromises several records at a high cost.

A study by BERR (2008) reveals that most organizations don't scan their outgoing communication for confidential information in order to prevent data leakage to unauthorized people. Email, instant message, webmail, website forms, file transfer or other electronic type of communication are unmonitored and uncontrollable once they leave the organization and dangerous if confidential data falls into the wrong hands (Blasco et al, 2012; Colwill, 2009). An insider can send confidential data to whomever they want since there are no security measures to prevent data from leaving the enterprise but rather to keep data out. Once the data has left the perimeter of the enterprise it can't be stopped from spreading and can end up anywhere and everywhere. An incident that happened in UK in 2012 consisted in a manager sending round an email containing a spreadsheet which stated the sexuality, ethnicity and disability status of the employees (Inside Housing, 2012).

2.2 Data leakage prevention

Data leakage prevention (DLP) is a technical solution against data leakage which monitor and filter outgoing communication according to confidential data (McCormick, 2008).

This is verified by Blasco and Jorge (2013) who explains that a DLP solutions works by analyzing, monitoring and controlling the usage of confidential data across computing systems in order to prevent intentional and accidental data leakage. ECS (2014) defines *monitoring*, *analysis* and *enforcement* as the following:

- Monitoring are referring to identifying confidential data in documents and other formats as well as locating enterprises contents, and either recording events or sending alarms when monitoring detects a breach towards the policy.
- Analysis refers to searching the content of files and analyzes them to file formats.
- Enforcement refers to using information gathered from monitoring to enforce the privacy of the enterprise data. Examples of this might be blocking access to cloud based storage platforms or blocking email sent by an employee that contains special keywords either in the text or in attachments.

Some DLPs creates a database of all known files in the organization, and scans them for keywords to tag them with a flag. If those files is seen trying to pass through the enterprise perimeter it will be blocked. Other solutions works by scanning all traffic passing through the firewall and scanning for keywords in real-time using deep packet inspection, so it even checks the content of the packet. A similar feature in all of these DLPs is the possibility to tag documents based on templates. If you have a document or presentation template that states the document is sensitive, it will not be allowed to pass the perimeter. Caputo et al. (2009) and Lawton (2008) argues that the DLP solution out on the market today still have many problems but that progress has been made to reduce false positive.

A DLP solution is supposed to prevent confidential data from leaking out of the enterprise (Blasco et al, 2012). By applying the enterprise policy to the DLP solution it is possible to to prevent certain data from leaving the enterprise in accordance to the policy as well as encrypting data which are leaving the enterprise (ECS, 2014). This would mean that a DLP solution could be tailored for each specific enterprise by preventing the data which they specify not to be able to leave the organization. The next generation firewalls normally have other features that work together with the DLP solution to prevent unauthorized usage of data, like Application Control that blocks different applications and webapps based on application ID instead of session TCP/UDP port. Many applications are evasive and run over TCP port 80 or 443, and if you block those ports you will end up blocking more or less the entire World Wide Web.

2.3 Information Systems Security Policies (ISSP)

The Information System Security Policy (ISSP) is a set of procedures created by senior management to help end users comply with the security standards which are necessary to secure the knowledge of the company and stay competitive (Von Solms & Von Solms, 2004). The ISSP is used to prevent data leakage and it is based on trust. A user reads, accepts and signs the ISSP, and if there is no monitoring or enforcement of the ISSP after this point, there might be a reason for data leakage.

It is also important that the users are compliant, they have to follow the guidelines and procedures stated in the ISSP. By only communicating the ISSP you are far from sure that the end users are compliant (Bulburgu, 2010; Von Solms & Von Solms, 2004). There are many reasons why a user isn't complying to the ISSP, but studies have shown that the main reason is that the ISSP isn't reflecting the current practices (Kolkowska & Dhillon, 2013). So if the organizations don't update their ISSP to reflect both the current practices and the current threats, they should consider their network and data as unsecure. The second reason that Lapke (2006) found for not complying to the ISSP is the resistance to security rules.

The same study also shows that more than 50% of the users in the organizations didn't know the current ISSP, and even worse was that most of the organization's security departments didn't know of this ignorance (Lapke, 2006). If the users don't know the ISSP, how can you expect the users to comply to it? If the ISSP is enforced the organization don't have to perform training every time a change is made, informing about the changes made is sufficient. If it is configured right the users can't be non-compliant, even if they don't know the current ISSP.

2.4 Insider Threat

During the last decades, enterprises has poured huge amounts of money and time into developing policies, binding arbitration agreements and security tools in order to secure their data storage from threats (Brendan, 2014). A recent study showed that 90% of the organization's security focuses on securing their data from external threats, while 70% of the frauds occurred within the enterprise (McCue, 2008). Recent studies in the field of data leakage have showed that organizations are increasingly worried about data leakage, unauthorized disclosure of sensitive and confidential data (Ahmad et al, 2013; Blasco et al, 2012; Colwill, 2009; Walker, 2008). By reviewing these studies you will find that there is a gap in the alignment of security implementations versus the actual threats. Enterprises are concerned about internal security breaches which occur more frequently compared to external security breaches, but they are focusing their security against external threats. In 2014 a case showed up in Iowa, USA. Two employees at the Iowa Human Services department used online storage for storing work related material which wasn’t allowed according to the ISSP. It took the IT Department 5 years to notice this breach, and no-one knows if the data stored at the online storage has been transferred somewhere else or abused during these 5 years (Databreaches, 2014).

Data leakage are usually caused by insiders, which are increasingly becoming a key concern for enterprises, because of their possibility to release classified data to unauthorized parties (Ahmad et al, 2013; Blasco et al, 2012, Colwill 2008). Insiders have the potential to cause greater harm to the organization and for a malicious user it comes with certain advantages compared to outside attacks (Colwill 2008). Studies states that insiders have privileged access to the enterprise data as well as knowledge of the infrastructure, the value of the data and how to cover the evidence of tampering (Ahmad et al, 2013; Blasco et al, 2012; Chivers et al, 2009; Colwill, 2009, Moore et al, 2009; Walker ,2008). These studies reveals that data leakage is mainly caused by insiders which already have legitimate access to confidential data because of their work. This would mean that the insiders has already passed the security mechanisms and can begin leaking data out of the enterprise when they see fit. With knowledge of the enterprise procedures it’s possible to erase the evidence of data leakage and avoid being found out by the enterprise. An incident was revealed during late 2014 where an employee at Memorial Hermann Health System had accessed medical records of approximately 10.600 patients over 7 years time. These records were accessed outside working hours, and as of now no-one knows what this data has been used for, or if it has left the organization (Roman, 2014).

Several studies imply that data leakage can occur through intentional or accidental acts by an insider (Annansingh,2005; Blasco et al, 2012, Colwill 2008). Data leakage which occurred by accident are often more severe compared to intentional data leakage (CSO, 2010 Blasco et al, 2012, Colwill 2008, Shabtai’s et al, 2012). In a survey with US banking and financial institutions, 91% of the organizations which took part in the survey claimed that they suffered financial loss where 30% of the cases resulted in 500.000 US dollars in loss or more (Randazzo et al., 2005). Another study performed by Kaspersky Labs shows that accidental data leakage has become a bigger concern than software errors when it comes to data leakage. 27% of the companies in that study had lost sensitive data during the last 12 months due to accidental information sharing. Only 20% had experienced data loss due to software vulnerabilities (Kaspersky, 2014).

Since most devices in the modern environment are connected to the Internet, a data leakage incident can result in unauthorized disclosure of confidential data to everyone. A single data leakage attack is enough to cause damage to the enterprise’s reputation and economics (Ahmad et al, 2013; Blasco et al, 2012; Colwill, 2009). A simple mouse click is enough for an insider to suddenly cause major damage to the organization. Lots of accidental Internet publishing accidents has happened. In Florida in 2012 a subcontractor to the Department of Children and Families, who was working on running background checks on employees to the department, stored all the data collected available on the Internet, with no kind of encryption on the data. It was available to everyone who could find it, no-one really knows if someone has gotten access to the data (WFTV, 2012).

2.5 Compliance and Intellectual Property

According to webspy (2009) there are two types of data which the enterprises need to protect in order to prevent data leakages; *regulatory compliance* and *intellectual property protection*.

- Regulatory compliance: Every enterprise is required to follow certain locally and internationally regulatory mandates by ensuring that private information, personally-identifiable information etc. are securely handled (webspy, 2009). Data leakage of personal information can have serious consequences if unauthorized parties get a hold of that information.
- Intellectual Property Protection: Protecting the enterprise important assets from those who try to steal confidential data and employees taking sensitive data are what data leakage prevention strives for (webspy, 2009). Assets which the enterprises have generated such as programs, formulas etc aren’t meant to leave the company premises, because it has ramifications on the enterprise itself. Once the asset leave the company

perimeter the company doesn't have control over the data anymore, nor the usage of it.

Enterprises can no longer afford to neglect the gap in the enterprise protection since data leakage can force the enterprise to violate compliance regulations which will affect the brand value considerable (Ahmad et al, 2013; Blasco et al, 2012; Rantala, 2008). Current network security solution doesn’t include data leakage prevention capabilities to prevent confidential data from leaving the enterprise (Kanagasingham, 2008). Data leakage solutions should address the protection of data in motion, rest and use (Blasco et al, 2012, Kanagasingham, 2008). Enterprises have a lot to lose if they don’t start to take the insider threat and data leakage seriously before it is too late and the damage is already done. This is the same for every enterprise, no matter the size. Every company is unique, either it produces something unique, is combining others products in a unique way, is doing a service at a unique price or other similar things that makes the company unique. If this uniqueness is shared with others, someone else can replicate the uniqueness and the first company might go out of business. Smaller companies cover smaller areas and have less to lose until it makes a difference, so it is just as important for them to secure their data as it is for larger enterprises.

Recent studies have revealed that cases of data leakages usually result on the loss of reputation, competitiveness and economic fees (Ahmad et al, 2013; Blasco et al, 2012). In 2007 25 million people lost their personal details in a single incident because the UK Government’s Revenue and Customs Department (HMRC) had an insider accident (Thomson, 2007). This could very well explain why insiders are so dangerous and why enterprises has become more concerned of data leakage as of lately. A single insider attack can result in data leakage of several sensitive data, causing great harm to the enterprise’s reputation and economic as well as the loss of sensitive client information. Another incident was made in South Carolina, USA, were an employee of the Department of health and human services got access to medicaid information on 228.000 persons and transferred that data to his personal email account. What that data was for and if it was used isn’t known (The State, 2012).

A study of 12 different security breaches from 2006 at larger American companies show that after a security breach the announcement of that breach result in a average company value drop of 1% (Goel & Shawky, 2009). One percent might seem like an insignificant number, but for a billion dollar company that is quite a lot. This makes it important to have an updated ISSP and perform enforcement of those procedures. Another study show indication that ISSP enforcement is a tool that significantly improves the data security within an organization (Knapp & Ferrante, 2012). The study shows that if you enforce the ISSP you automatically have the possibility to perform policing, you will get a report of who has tried to perform a task that is a breach of the current ISSP and have the possibility to punish users if given factors are taken into account (Ibid).

The assumed outcome of non-compliance is an important factor when it come to user behaviour and significantly affect the user's choices and attitude. If a user thinks there will be no negative effects to an exposed security breach, he may not think twice before bending the rules and regulations. And severity of the incident is more important than the certainty to get caught (Bulburgu, 2010; D’Arcy, Hovav & Galletta, 2009; Son, 2011). On the other hand, if a user knows he will get caught and there is a punishment for breaking the rules, studies show that most users will stay compliant. But the same study shows that if there is a reward-system for those who are compliant it will be an important factor for building up a better organization security culture (Chen, Ramamurthy, & Wen, 2012).

O'Connor (2014) stated in his study that modern people cannot give up on their electricity, electronic devices, internet etc. because they enable the people to perform better in a shorter time. It’s therefore not an available option to remove all electronics, but confidential data must still be secure. Modern people are a threat to confidential data because of all the electronic devices (O'Connor, 2014; Blasco et al., 2012; Colwill, 2009; Kavanagh, 2006). People bring their laptop online through insecure networks, plugging in flash drives which had virus, all in all accidents which can cause great damage on the enterprise. Colwill (2008) state that by encrypting confidential data it is possible to avoid detection when the DLP monitoring the data doesn’t have the decryption key.

Implementing technical solutions can help you reduce data leakage, but they can also have negative effects. One thing is that false positives will take time and the users will try to bypass the security if it doesn't work as supposed or it is a hassle to use it. A survey performed in 2006 shows that 34% of all respondents say that security measures interfere with their job tasks. (Post & Kagan, 2007) This shows that implementing security is something that should be taken seriously, the organization have to make sure it is aligned with the ISSP and that it is communicated.

Chapter III

3. Theoretical background

3.1 Theory of planned behavior

The theory of planned behavior (TPB) is a predictive persuasion theory published by Ajzen (1991) and is an extension of the theory of reasoned action (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975). Ajzen (1991) stipulates that the TPB can predict the individual's intention to perform certain behaviors by analyzing the individual's attitude, subjective norms and perceived behavioral control towards the behavior. The topics which makes up the theory of planned behavior is described as the following by Ifinedo (2011):

Topic	Description
Attitude	the degree to which an individual feels towards a specific behavior, in the case of this research the attitude towards complying with the ISSP.
Subjective norms	the perceived social pressure of what people around the individual thinks about a given behavior, in the case of this research, the requirements of the ISSP.
Perceived behavior control	(influenced by the social-efficacy from Bandura (1977, 1992, 1997) in the social cognitive theory) the individual's assessment on their performance of a certain behavior, in the case of this research, the individual's judgment of their assets against filling in the requirements of the ISSP.

Table 1: Ifinedo (2011) description on the contents of TPB

The theory of planned behavior is today one of the most widely used predictive persuasion theories and it has been used across several different research topics (Ifinedo, 2011). The theory of planned behavior has also been used in the field of information security and information system security policy (ISSP) and used in several studies such as the ones by

Venkatesh et al. (2003), Bulgurcu et al. (2010), Lee & Kozar (2005), Leonard et al. (2004). Several studies which have used the theory of planned behavior have concluded that attitude, subjective norms and perceived behavior control has influenced the individual's intent to comply with ISSP (Ifinedo, 2011; Venkatesh et al., 2003; Bulgurcu et al.,2010; Lee & Kozar, 2005; Leonard et al., 2004)

Venkatesh et al. (2003) used a combination of several models in their study in order to formulate and empirically validate a unified theory of acceptance and use of technology (UTAUT). The models which was included in the study was the theory of reasoned actions (TRA), technology acceptance model (TAM), motivational model (MM), theory of planned behavior (TPB), combined TAM and TPB (C-TAM-TPB), model of PC-utilization (MPCU), innovation diffusion theory (IDT) and social cognitive theory (SCT). The result was a successful tool which could predict the likelihood of individuals being compliant (Venkatesh et al., 2003).

Bulgurcu et al. (2010) wanted to identify the factors which affect the individuals to be compliant with the ISSP in order to protect the information and technical resources of the companies. Rational Choice Theory was therefore integrated with the theory of planned behavior. The outcome of the study showed that attitude, normative beliefs, and self-efficacy affect the individual's intent to comply and that ISA has a positive effect on the individual's attitude and outcome beliefs (Bulgurcu et al. (2010).

The study by Lee & Kozar (2005) combined the theory of planned behavior with innovation diffusion theory and IT ethics and morality. The purpose of the research was to understand why individuals don't use anti-spyware programs despite the threats which exist by doing an empirical investigation of factors which affect the individual's decision to use anti-spyware software. The conclusion demonstrated that the adaptation of anti-spyware software was affected by the individual's attitude, subjective norm, perceived behavioral control, and denial of responsibility. Other factors such as moral obligation ease of use, and perceived cost affected the individual’s intention to adopt less than what was believed (Lee & Kozar, 2005)

Leonard et al. (2004) on the other hand combined the theory of planned behavior with the theory of reasoned action and ethical decision-making models. The research was to extend the study of ethical behavior in the field of IT by develop and test an ethical behavioral model. The result showed that attitude and behavioral intention are affected by certain factors while other depends on the scenario and that organizations should consider adopting trainings to avoid undesired misuses (Leonard et al., 2004).

3.2 Security awareness

Several studies imply that data leakage can occur through intentional or accidental acts by an insider (Annansingh,2005; Blasco et al, 2012, Colwill 2008; CSO, 2010; Shabtai’s et al, 2012). Data leakage which occurred by accident are often more severe compared to intentional data leakage (CSO, 2010 Blasco et al, 2012, Colwill 2008, Shabtai’s et al, 2012). Modern organizations try to encourage the work practices through teamwork and shared responsibility and are reliable on trust and information sharing. However, the US Federal Information Processing Standards (FIPS) states that individual ownership increases accountability and through audit trailing it also reduces illicit usage (Adams & Sasse, 1999).

Individuals tend to be not sufficiently informed about the security issues that exist around them self. (Adams & Sasse, 1999; Bulgurcu et al, 2010). This has caused the individuals to develop their own view of possible security threats and the importance of security which are often very inaccurate to the real issue. An employee’s security awareness may be built from personal experience such as being attacked by virus or didn’t follow the security rules and regulations, or it can be built on external sources of information such as newspaper, journals etc (Bulgurcu et al, 2010). According to Whitman et al. (2001), the best way to ensure that the individuals are compliant with the ISSP is to make them understand and accept necessary guidelines.

Many researchers and best practice have said that there are many benefits of security education and training initiatives (D'Arcy et al, 2009). Several researchers have discussed the necessity of SETA program to decrease the amount of potential data leakages (Dhillon 1999, Parker 1998, Whitman 2004). The information security awareness is meant to be the employee's compliance to the information security policy and is a very important part of an effective information security management program (Bulgurcu et al, 2010). The user awareness of security policies; security education, training, and awareness (SETA) programs and monitoring is a security countermeasures meant to reduce information security misuses, intentions to misuse and unintentional accidents by the users (Bulgurcu et al, 2010; D'Arcy et al, 2009). If the users are aware of the security policies, educated in the risks, trained in how to handle the risk and what happens if they aren't compliant, they might become more interested and deeper themselves in information technology more deeply and how difficult it is to detect misuse incidents.

3.2 Conceptual framework for Research

In order to explore how data leakage occur despite ISSP being implemented, we based our research model on the theory of planned behavior to see if it is the employee's intention to comply with the ISSP that's the cause of the data leakage. However, the theory of planned behavior doesn't take the unintentional data leakage into account, something which earlier studies have presented to an equal or even greater threat than intentional data leakage. While the theory of planned behavior works to identify if an individual is or isn't following the ISSP, there is still the issue of unintentional data leakage which earlier studies has described as the lack of awareness. We therefore proposed a research model based on the TPB as a cause for intentional data leakage combined with the lack of awareness which leads to unintentional data leakage (figure 1).

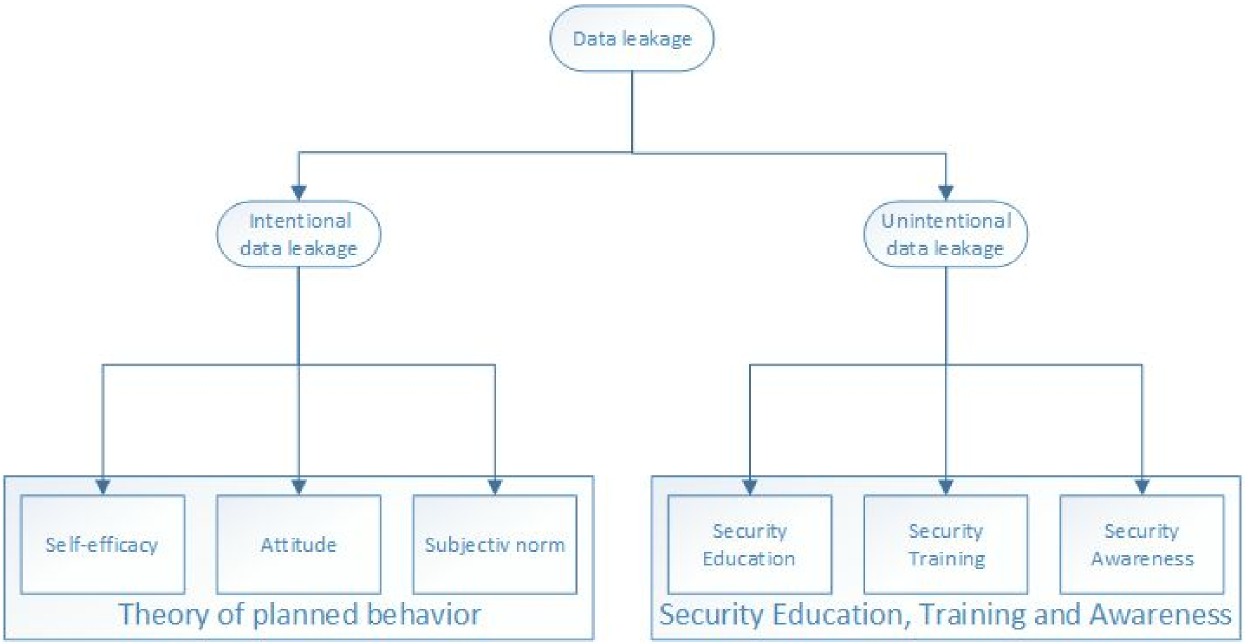


Figure 1: Proposed research model

Subjective norms are the motivation of an individual to comply with a certain act which is heavily influenced by other people's behaviors through observations or consultation (Ajzen, 1991). An individual's behavior can therefore be influenced by what the people around the individual are behaving. In regards to the compliancy of the ISSP in organizations, individuals are prone to be influenced by their superiors, co-workers or subordinates if they are show signs of following the ISSP (Chan et al.,2005). In accordance with the studies by Lee and Larsen (2009), Pahnila et al. (2007), Bulgurcu et al. (2010), and Herath and Rao (2009), ISSP compliance is heavily affected by the subjective norms.

TPB suggest that an individual's behavioral intentions are a cause of the individual's attitude (Ajzen, 1991). Its therefore beneficial for the organization and the individual alike that the individual has a positive attitude. In regards to compliance of ISSP, individuals with a positive attitude towards the organization's ISSP are more likely to abide by those rules, guidelines and requirements (Sasse et al., 2004; Ng et al., 2009; Herath and Rao,2009a; Bulgurcu et al., 2010). This also works the other way around were individuals with negative attitude are more likely to not follow the ISSP (Pahnila et al., 2007; Myyry et al., 2009). Recent studies about the compliance with the acceptable IS has showed that attitude has an impact on behavioral intentions (Bulgurcu et al., 2010; Pahnila et al., 2007; Myyry et al., 2009; Herath and Rao, 2009).

Self-efficacy implies an individual's capabilities to handle a certain task or make a decision by evaluating their own competence (Ajzen, 1991; Bandura, 1977, 1991). Studies in the field of ISSP has showed that individuals with higher competence with IS will be more complying with the ISSP compared to those of lesser competence (Compeau and Higgins, 1995). It is expected that individuals with higher IS security capabilities and competence understands the need to follow the ISSP. Studies has showed that self-efficacy is relevant to ISSP compliance and it will affect the behavior intention.

Security education is meant to educate the individuals their roles and responsibilities regarding the risks and threats related to information security (Bulgurcu et al., 2010). By education the individuals about the threats there are more prone to avoid doing mistakes and by educating them about their responsibility they will know the consequences of not being compliant with the ISSP. With the help of monitoring, it is possible to prevent intentional data leakage if the individuals know that they are hold responsible for their own actions (D'Arcy et al, 2009).

To ensure that the individuals are acting in accordance with the information security rules and regulations, security training needs to be provided to ensure that the individuals are compliant with the ISSP (Bulgurcu et al., 2010). Adequate training can therefore prevent a lot of accidental data leakage by training the individuals on how they should perform their work while being compliant with the ISSP. The purpose of security training is to develop relevant security skills and competencies to support job performance (Bulgurcu et al., 2010; D'Arcy et al, 2009).

The objective of security awareness is to ensure that the individuals are aware of the threats and risks related to information security (Bulgurcu et al., 2010; D'Arcy et al, 2009). Its focus is the individual's attention on security and consequences of not being compliant with the ISSP. Individuals with higher security awareness are prone to provide better security practice since they are aware of the risks, their responsibility and how to handle it (Bulgurcu et al., 2010; D'Arcy et al, 2009; Dhillon, 2006).

Chapter IV

4. Research Methodology

The purpose of this chapter is to give an understanding on the general research methodology used in this study as well as the tools used in the data collection and analysis.

4.1 Research Approach

According to Creswell (2013) there are three kinds of research approaches; *Quantitative*, *Qualitative* and *Mixed method* approach.

Quantitative research involves deductive testing of objective theories by examining the relationship through measurable data which can be analyzed using statistical procedures. The final report will also have a pre-defined structure containing introduction, literature and theory, methods, results, and discussion. The findings of this type of research are often generalized in order to be replicated (Ibid). Quantitative research approaches are therefore more suited in those researches which focus on measurable data and being able to replicate the findings.

Qualitative research involves inductive exploring of a problem in order to understand the issue described by individuals or groups. The final report has a flexible style compared to the report of a quantitative research which has a predefined structure. The findings of this type of research should render the complexity of a situation (Ibid). Qualitative researches are therefore more suited for those researches which try to gain a deeper understanding of a complex situation.

Mixed method research involves the combination of qualitative and quantitative approaches in order to give a more complete understanding of a problem which either approach cannot provide alone. This approach often uses distinct designs which might include philosophical assumptions and theoretical frameworks (Ibid). Mixed method research are more suited in those researches which want to have the best of the both approaches and gain an even deeper understanding of a situation or problem.

In this research we decided to use the theory of planned behavior (TPB) and SETA to identify why data leakage occur despite the implementation of ISSP. TPB has been used in earlier studies to identify the individual's intention to comply with the ISSP, but as other studies has shown, accidental data leakage can occur even if the individuals are not compliant with the ISSP. Therefore our theoretical framework will combine TPB with SETA to identify whether the accidental data leakage is caused by the lack of security awareness or intentional data leakage caused by malicious individuals.

Based on the information above about the different research approaches, we chose to do this research as a qualitative research. The purpose of this research is to understand the current state of data leakage in organizations. We wanted to dig deeper into this issue by looking into two different companies which are susceptible to data leakage and how they handle sensitive data. The data collection in this research are based on personal interviews, documentation and live traffic analysis in order to understand how sensitive data is handled. Due to the data collection method being qualitative, a quantitative research method could therefore not be applied to this research.

4.2 Research Purpose

According to Baxter & Jack (2008) the research purpose is used to explain the overall study whether it is describing a case, explore a case or compare between cases. Yin (2003) defines this as *explanatory*, *exploratory*, or *descriptive* research purposes.

Explanatory is used when you try to explain presumed causal links in real-life interventions which are too complex for surveys or experimental strategies (Baxter & Jack, 2008; Yin, 2003). In other words to clarify why and how there is a relationship between variables

Exploratory is used when the situation which is being evaluated doesn't have a clear, single set of outcomes (Ibid). It can therefore be used to identify and obtain information by giving insight on a particular problem.

Descriptive is used to describe the phenomena and the real life context in which it occur (Ibid). In other words descriptive research purpose is useful for explaining the characteristics as it is observed.

In this research we have been looking into what kind of data leakages exists within the studied organizations and technically how the leakage is performed. We wanted to see if there is a need to enforce IT Security Policies, or if it is worth the hassle. There is a relatively high cost and quite a lot of work to tune it to work as good as possible, and we have to review the reported breaches manually to ensure what has happened is in fact a data leakage.

The purpose of this research is to explore how organizations are experiencing data leakages despite policies being implemented. The idea is to get an understanding of what data leakage is, how it occur and give an insight to how policy enforcement can prevent data leakage. Overall, the purpose of this research is exploratory which are used to get a deeper understanding.

4.3 Research Strategy

There exist five different research strategies and each of them have their own weaknesses and strengths; *experiments, research survey, archival analysis, histories* and *case studies*. Each of these strategies can be used for all three of the research purposes; exploratory, descriptive, and explanatory (Yin, 2003). Its therefore possible to choose any of these five strategies since this research are using an exploratory approach.

However, in our research neither experiments, research surveys, archival analysis nor histories is well suited, based on our data collection method and is therefore not applicable for this research.

Case study is a qualitative approach which involves exploring through one or more cases. The cases are studied in great detail and data is collected from multiple sources of information in order to form a case description and case theme (Creswell, 2013). A case study is therefore a research strategy, which is a way of collecting and analyzing data. According to Creswell (2013) there exist three different variations of case study; single instrumental, multiple and intrinsic case study.

- *Single instrumental case study* involves illustrating the issue by a single case
- *Multiple case study* involves illustrating the issue through multiple case studies.
- *Intrinsic case study* involves studying the case itself as it presents unusual and unique situation (Creswell, 2013).

This research focuses on “*how organizations are experiencing data leakages despite policies being implemented”* and is utilizing a case study performed within three different organizations. Since three similar case studies is performed in three different organizations, this research is following a multiple case study strategy rather than a single instrumental case study strategy. By doing the same case study in three different organizations we can compare and triangulate patterns to get a more reliable result.

4.4 Data Collection Method

One important feature about case study is the use of multiple data sources which in turn improves the credibility of the research (Yin, 2003). By using several sources it is also possible to get a better understanding of the issue compared to what a single source would give. Some data sources includes documentation, archival records, interviews, physical artifacts, direct observations, and participant-observation (Baxter & Jack, 2008).

In this research we decided to use documentation by collecting the company’s IS security policy since it builds the foundation of the research. The reason for this is to gather better knowledge of the organization, what data they consider sensitive, how they handle this sensitive data and how they have handled previous breaches of sensitive data, if any. The result of the documentation analysis also gave us a baseline on what data to look for when performing the traffic analysis. As an example, if the policy said personally identifiable information is sensitive, we created a filter that searches for social security numbers in the data leaving the company. When going through the policies we also searched for evidence of any SETA process in order to see if they handled awareness to prevent any unintentional data leakage, according to our theoretical framework.

Direct observation has also been used in this research since it covers what is actually happening within the organization. In order to perform a direct observation of data leakage we chose to do a traffic analysis by placing a deep inspection firewall in parallel with the organization's current firewall. This parallel firewall has gathered all information that was passing through the company’s perimeter and searched for keywords in the data without disrupting the organization's business. This firewall was installed on a mirror port of the existing firewall, so it was not performing any active decision based on the data, just listening and analyzing the data it received. It looked into the data of the packets and looked for predefined keywords, which are based on the interviews and best practice. As an example, if the ISSP states BitTorrent is illegal according to policy, that event will be tracked. But we also wanted to cover what kind of data is shared in the BitTorrent session. Was it sensitive data that was shared? Or was it just someone downloading some freeware tool from the Internet? Based on the type of event we made assumptions on the event to categorize them as intentional or unintentional, based on our theoretical framework.

We also did interviews focused on the company's existing measures taken to limit data leakage and their IS Security policies. Examples of questions is if they have a defined role that is responsible for updating the ISSP, how do they perform updates and how are users made aware of the changes made. We also tried to cover if they have had any known data breaches and how they handled or planned to handle such events. We also tried to cover what kind of data is most important within the company, what they have to secure most, and how it is secured as of today. The main reason for the interview is to get to know the company better and to map types of data to the IS Security policy and to our data collection strategy, as well as uncovering their SETA strategy. The SETA strategy was important for us to get knowledge of the awareness of the employees, to be able to follow our theoretical framework.

4.5 Analysis Plan

The purpose of data analysis is categorizing, tabulating or in some other way combine the evidence to answer the initial purpose of the research (Yin, 1994). The focus in this phase of the case study is to evaluate the gathered data from the earlier stage of the research, the data collection phase. Yin (2003) presents five analytic techniques which could be used to analyze the collected data: *pattern-matching*, *explanation building*, *time series analysis, logic model* and *cross case synthesis.*

pattern-matching is one of the most desirable analysis techniques which involves comparing empirically based pattern with a predicted pattern. The case study can gain validity of the patterns match each other but the patterns can also be relevant even if they don’t match (Ibid). Pattern matching is there for useful to find simple patterns and to ensure that what earlier studies have shown is actually correct or finding conflicts which don’t match the patterns.

cross case synthesis is specifically developed for multiple cases study and is mostly suited when there are two or more cases. The analysis and the findings are likely to be easier and more robust than having a single case (Ibid). The previous four techniques appear to be limited to single cases studies while this technique is designed for multiple case studies specifically. Having more cases to analyses can give a more robust result.

The interviews was similar for all companies, there was a basic set of questions that was asked during all interviews. The answers was written down and accepted by the interviewee prior to being used in the research. The answers was compared to the existing IS Security policy using pattern-matching. Since all companies in the research should be comparable and have the same vision for security, we also compared the different company's answers and IS Security policy using pattern matching. Pattern matching was used to see if there is a different opinion on what data is important and how to secure data even among similar companies.

The traffic analysis was performed using a unified threat management firewall with application visibility and data loss protection. One important thing with this firewall is that it can generate log events based on different triggers that we define. We defined a rule base that triggered on events that is non-compliant to the IS security policy or where packets are consisting of important data or knowledge that shouldn't be leaked. As an example, if a company says that source code is sensitive, and it should never leave the company premises, we created a trigger that searched for source code in the data leaving the company and create an event based on that. We used a tool that can generate a report based on those logged events, and that report was used as input to our traffic analysis. Most next-generation firewalls can create such a report, but there can be false positives and data that have to be explained. We used the report as a starting point to dig deeper into the events that were interesting for the research, using explanation-building analysis technique. An example to this could be that if an event was registered for source code leakage, we looked deeper into this event. Maybe it is just a user that has asked a general question to a forum, attaching a bit of general code to be able to solve a task.

The theory of planned behavior stipulates that an individual's intent to comply with the ISSP is caused by three factors, however it does not apply to unintentional data leakage. Therefore we believe that unintentional data leakage is caused by other factors, ones which SETA might cover. By cross analysing the data collected from the organizations it is possible to identify whether the data leakages are intentional or unintentional data leakage based on our conceptual framework.

Chapter V

5. Data collection

5.1 Information on tool used

To perform the traffic analysis we used a Checkpoint firewall that was installed in tap mode on a mirrored port in the switch where the company's existing firewall external interface was connected. By doing that we were feeding the installed Checkpoint firewall with the same data as the existing firewall in both outbound and inbound directions.

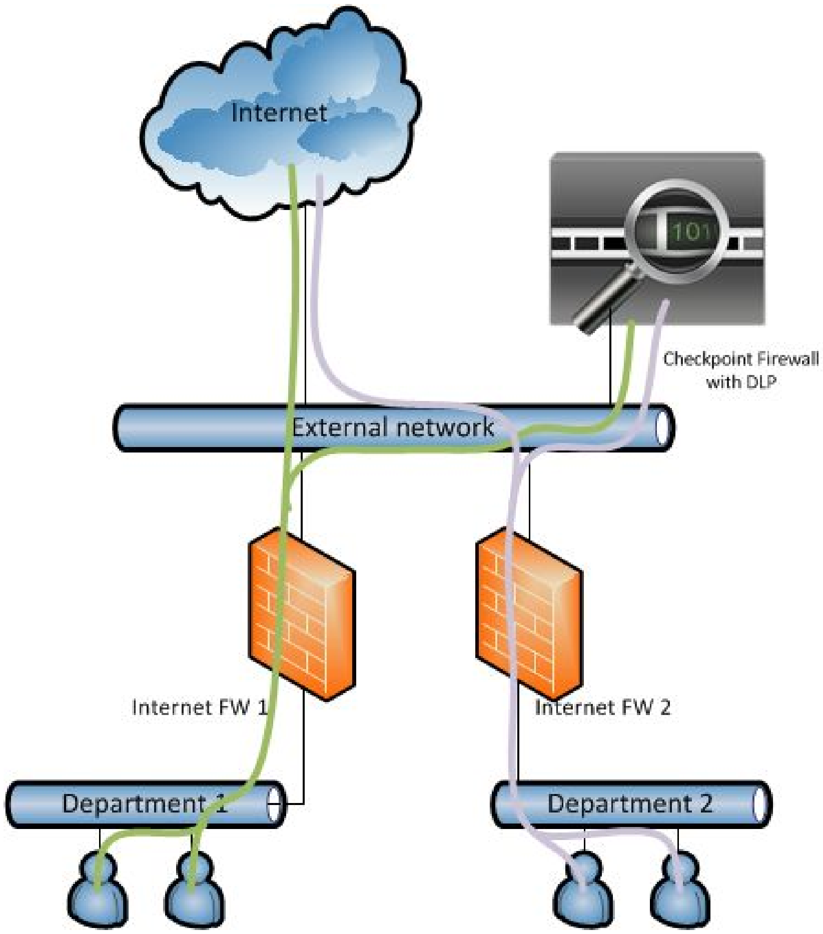
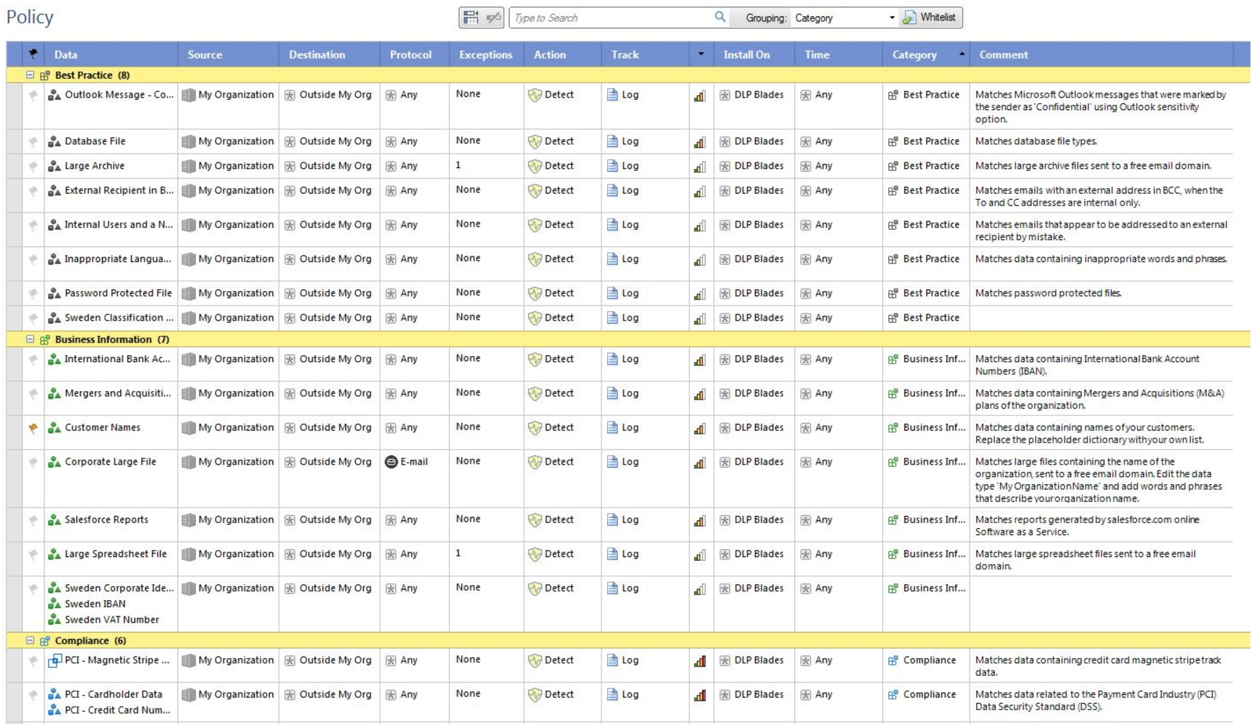


Figure 2: Conceptual network drawing of DLP implementation for data collection

This firewall was configured to allow all traffic and just register the data that was passing, it did not make any enforcement and was not interfering with the daily business at the companies where we installed it.

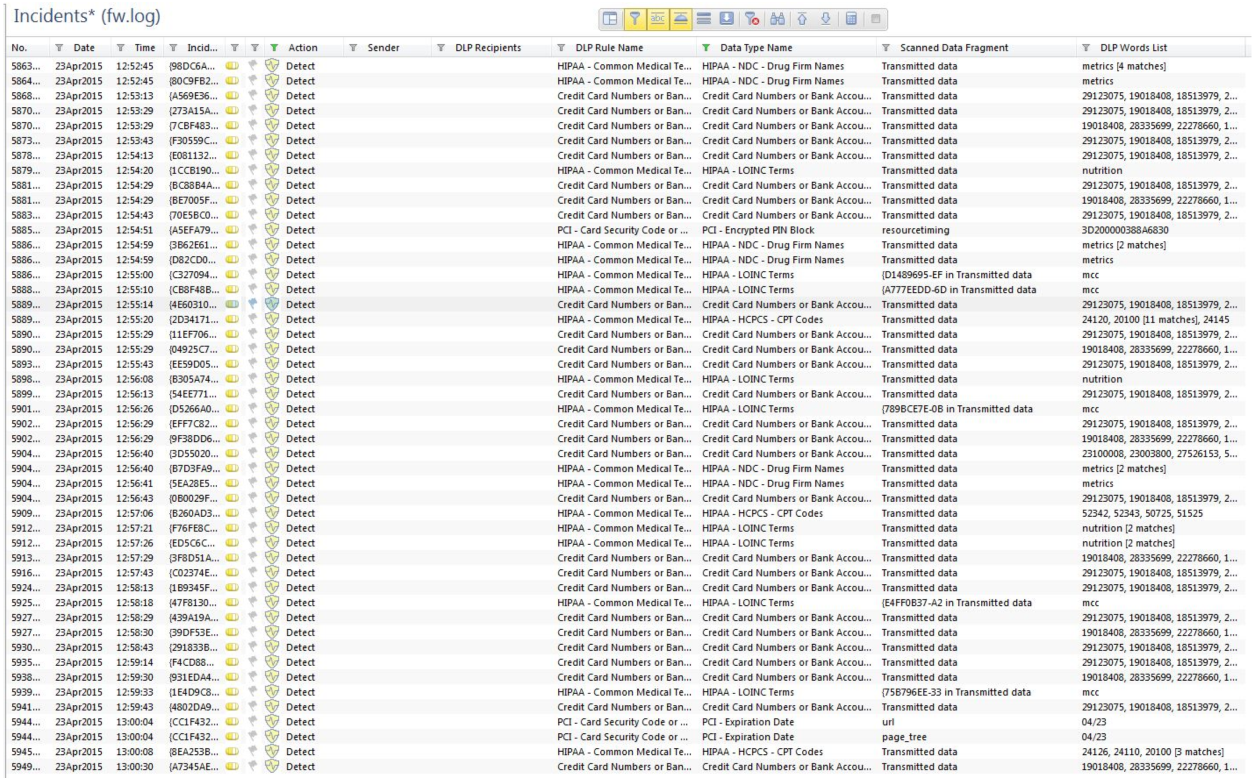
We did create a rulebase that was based on the ISSP to trigger information based on the traffic that was received. We also did enter some best practice triggers on the firewall, so that we could catch those incidents too. These best practice triggers was e.g. credit card numbers, medical information and large files. All of the data that is registered will be placed in a category like Business information, Compliance, Personally Identifiable Information etc.



Data	Source	Destination	Protocol	Exceptions	Action	Track	Install On	Time	Category	Comment
⊟ Best Practice (8)										
Outlook Message - Co...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Best Practice	Matches Microsoft Outlook messages that were marked by the sender as 'Confidential' using Outlook sensitivity option.
Database File	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Best Practice	Matches database file types.
Large Archive	My Organization	Outside My Org	Any	1	Detect	Log	DLP Blades	Any	Best Practice	Matches large archive files sent to a free email domain.
External Recipient in B...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Best Practice	Matches emails with an external address in BCC, when the To and CC addresses are internal only.
Internal Users and a N...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Best Practice	Matches emails that appear to be addressed to an external recipient by mistake.
Inappropriate Langua...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Best Practice	Matches data containing inappropriate words and phrases.
Password Protected File	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Best Practice	Matches password protected files.
Sweden Classification ...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Best Practice	
⊟ Business Information (7)										
International Bank Ac...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Business Inf...	Matches data containing International Bank Account Numbers (IBAN).
Mergers and Acquisiti...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Business Inf...	Matches data containing Mergers and Acquisitions (M&A) plans of the organization.
Customer Names	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Business Inf...	Matches data containing names of your customers. Replace the placeholder dictionary withyour own list.
Corporate Large File	My Organization	Outside My Org	E-mail	None	Detect	Log	DLP Blades	Any	Business Inf...	Matches large files containing the name of the organization, sent to a free email domain. Edit the data type 'My OrganizationName' and add words and phrases that describe your organization name.
Salesforce Reports	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Business Inf...	Matches reports generated by salesforce.com online Software as a Service.
Large Spreadsheet File	My Organization	Outside My Org	Any	1	Detect	Log	DLP Blades	Any	Business Inf...	Matches large spreadsheet files sent to a free email domain.
Sweden Corporate Ide... Sweden IBAN Sweden VAT Number	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Business Inf...	
⊟ Compliance (6)										
PCI - Magnetic Stripe ...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Compliance	Matches data containing credit card magnetic stripe track data.
PCI - Cardholder Data PCI - Credit Card Num...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Compliance	Matches data related to the Payment Card Industry (PCI) Data Security Standard (DSS).

Figure 3: DLP policy

The firewall then creates a log of the incidents based on the triggers created. This list includes information from a deep packet inspection that is performed for every single packet that is passing through the firewall. It will search through data transmitted, attachments, data entered into forms and everything that can be represented as text.

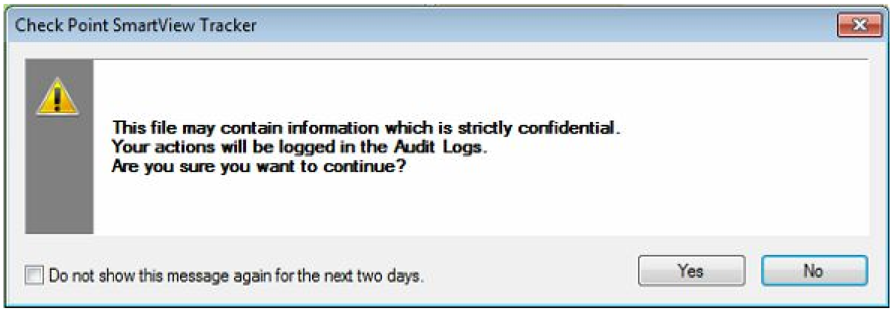


Incidents* (fw.log)

No.	Date	Time	Incid...			Action	Sender	DLP Recipients	DLP Rule Name	Data Type Name	Scanned Data Fragment	DLP Words List
5863...	23Apr2015	12:52:45	{98DC6A...			Detect			HIPAA - Common Medical Te...	HIPAA - NDC - Drug Firm Names	Transmitted data	metrics [4 matches]
5864...	23Apr2015	12:52:45	{80C9FB2...			Detect			HIPAA - Common Medical Te...	HIPAA - NDC - Drug Firm Names	Transmitted data	metrics
5868...	23Apr2015	12:53:13	{A569E36...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5870...	23Apr2015	12:53:29	{273A15A...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5870...	23Apr2015	12:53:29	{7CBF483...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	19018408, 28335699, 22278660, 1...
5873...	23Apr2015	12:53:43	{F30559C...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5878...	23Apr2015	12:54:13	{E081132...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5879...	23Apr2015	12:54:20	{1CCB190...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	Transmitted data	nutrition
5881...	23Apr2015	12:54:29	{BC88B4A...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5881...	23Apr2015	12:54:29	{BE7005F...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	19018408, 28335699, 22278660, 1...
5883...	23Apr2015	12:54:43	{70E5BC0...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5885...	23Apr2015	12:54:51	{A5EFA79...			Detect			PCI - Card Security Code or ...	PCI - Encrypted PIN Block	resourcetiming	3D200000388A6830
5886...	23Apr2015	12:54:59	{3B62E61...			Detect			HIPAA - Common Medical Te...	HIPAA - NDC - Drug Firm Names	Transmitted data	metrics [2 matches]
5886...	23Apr2015	12:54:59	{D82CD0...			Detect			HIPAA - Common Medical Te...	HIPAA - NDC - Drug Firm Names	Transmitted data	metrics
5886...	23Apr2015	12:55:00	{C327094...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	{D1489695-EF in Transmitted data	mcc
5888...	23Apr2015	12:55:10	{CB8F48B...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	{A777EEDD-6D in Transmitted data	mcc
5889...	23Apr2015	12:55:14	{4E60310...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5889...	23Apr2015	12:55:20	{2D34171...			Detect			HIPAA - Common Medical Te...	HIPAA - HCPCS - CPT Codes	Transmitted data	24120, 20100 [11 matches], 24145
5890...	23Apr2015	12:55:29	{11EF706...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5890...	23Apr2015	12:55:29	{04925C7...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	19018408, 28335699, 22278660, 1...
5893...	23Apr2015	12:55:43	{EE59D05...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5898...	23Apr2015	12:56:08	{B305A74...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	Transmitted data	nutrition
5899...	23Apr2015	12:56:13	{54EE771...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5901...	23Apr2015	12:56:26	{D5266A0...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	{789BCE7E-0B in Transmitted data	mcc
5902...	23Apr2015	12:56:29	{EFF7C82...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5902...	23Apr2015	12:56:29	{9F38DD6...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	19018408, 28335699, 22278660, 1...
5904...	23Apr2015	12:56:40	{3D55020...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	23100008, 23003800, 27526153, 5...
5904...	23Apr2015	12:56:40	{B7D3FA9...			Detect			HIPAA - Common Medical Te...	HIPAA - NDC - Drug Firm Names	Transmitted data	metrics [2 matches]
5904...	23Apr2015	12:56:41	{5EA28E5...			Detect			HIPAA - Common Medical Te...	HIPAA - NDC - Drug Firm Names	Transmitted data	metrics
5904...	23Apr2015	12:56:43	{0B0029F...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5909...	23Apr2015	12:57:06	{B260AD3...			Detect			HIPAA - Common Medical Te...	HIPAA - HCPCS - CPT Codes	Transmitted data	52342, 52343, 50725, 51525
5912...	23Apr2015	12:57:21	{F76FE8C...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	Transmitted data	nutrition [2 matches]
5912...	23Apr2015	12:57:26	{ED5C6C...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	Transmitted data	nutrition [2 matches]
5913...	23Apr2015	12:57:29	{3F8D51A...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	19018408, 28335699, 22278660, 1...
5916...	23Apr2015	12:57:43	{C02374E...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5924...	23Apr2015	12:58:13	{1B9345F...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5925...	23Apr2015	12:58:18	{47F8130...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	{E4FF0B37-A2 in Transmitted data	mcc
5927...	23Apr2015	12:58:29	{439A19A...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5927...	23Apr2015	12:58:30	{39DF53E...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	19018408, 28335699, 22278660, 1...
5930...	23Apr2015	12:58:43	{291833B...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5935...	23Apr2015	12:59:14	{F4CD88...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5938...	23Apr2015	12:59:30	{931EDA4...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	19018408, 28335699, 22278660, 1...
5939...	23Apr2015	12:59:33	{1E4D9C8...			Detect			HIPAA - Common Medical Te...	HIPAA - LOINC Terms	{75B796EE-33 in Transmitted data	mcc
5941...	23Apr2015	12:59:43	{4802DA9...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	29123075, 19018408, 18513979, 2...
5944...	23Apr2015	13:00:04	{CC1F432...			Detect			PCI - Card Security Code or ...	PCI - Expiration Date	url	04/23
5944...	23Apr2015	13:00:04	{CC1F432...			Detect			PCI - Card Security Code or ...	PCI - Expiration Date	page_tree	04/23
5945...	23Apr2015	13:00:08	{8EA253B...			Detect			HIPAA - Common Medical Te...	HIPAA - HCPCS - CPT Codes	Transmitted data	24126, 24110, 20100 [3 matches]
5949...	23Apr2015	13:00:30	{A7345AE...			Detect			Credit Card Numbers or Ban...	Credit Card Numbers or Bank Accou...	Transmitted data	19018408, 28335699, 22278660, 1...

Figure 4: Log of triggered events

From that list you can take a closer look at one single incident to analyse it further whether it is a real incident or a false positive. What we have learnt by doing this is that this part is really important for a security administrator to perform to be able to tune the information so you only get the real incidents in the log. When you take a closer look at the incident it will be logged in an audit log since you can gather sensitive data from this and even read mail conversations or attachments. This also means you have to have a security policy for who can access these logs and how to handle them. These logs are really sensitive.



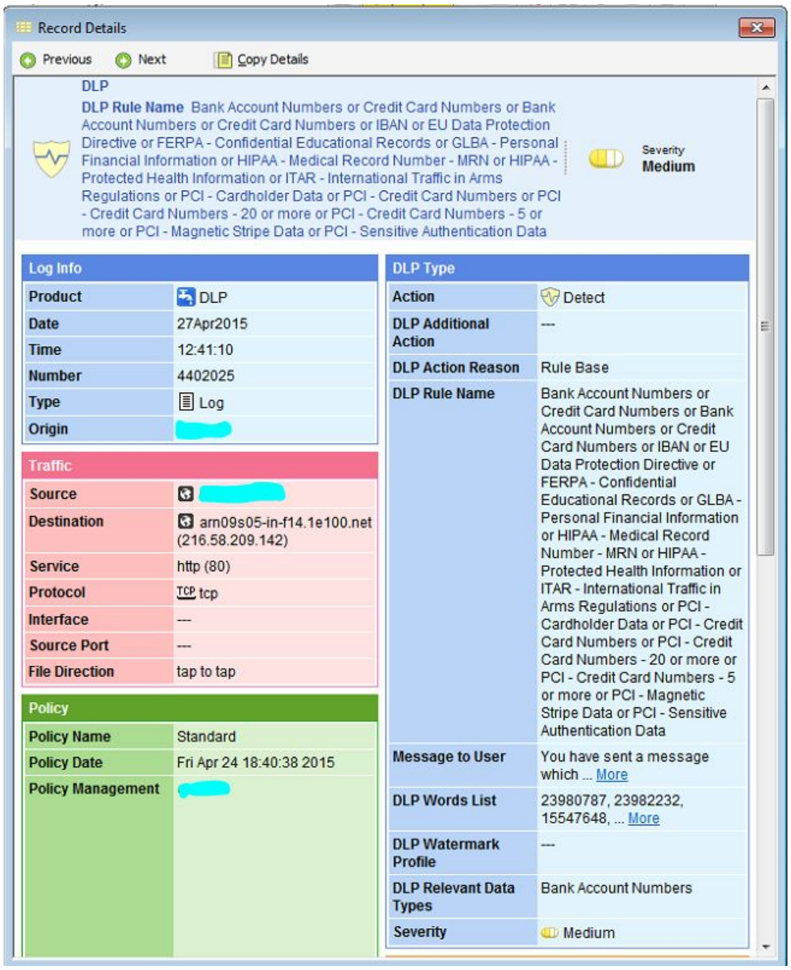
Check Point SmartView Tracker

This file may contain information which is strictly confidential.
Your actions will be logged in the Audit Logs.
Are you sure you want to continue?

□ Do not show this message again for the next two days.

Figure 5: Information pop-up for administrator audit logging

The closer look at the data reveals all information on what kind of data has been sent, at what time, by who and to where.



DLP

DLP Rule Name Bank Account Numbers or Credit Card Numbers or Bank Account Numbers or Credit Card Numbers or IBAN or EU Data Protection Directive or FERPA - Confidential Educational Records or GLBA - Personal Financial Information or HIPAA - Medical Record Number - MRN or HIPAA - Protected Health Information or ITAR - International Traffic in Arms Regulations or PCI - Cardholder Data or PCI - Credit Card Numbers or PCI - Credit Card Numbers - 20 or more or PCI - Credit Card Numbers - 5 or more or PCI - Magnetic Stripe Data or PCI - Sensitive Authentication Data

Severity **Medium**

Log Info	
Product	DLP
Date	27Apr2015
Time	12:41:10
Number	4402025
Type	Log
Origin	[redacted]

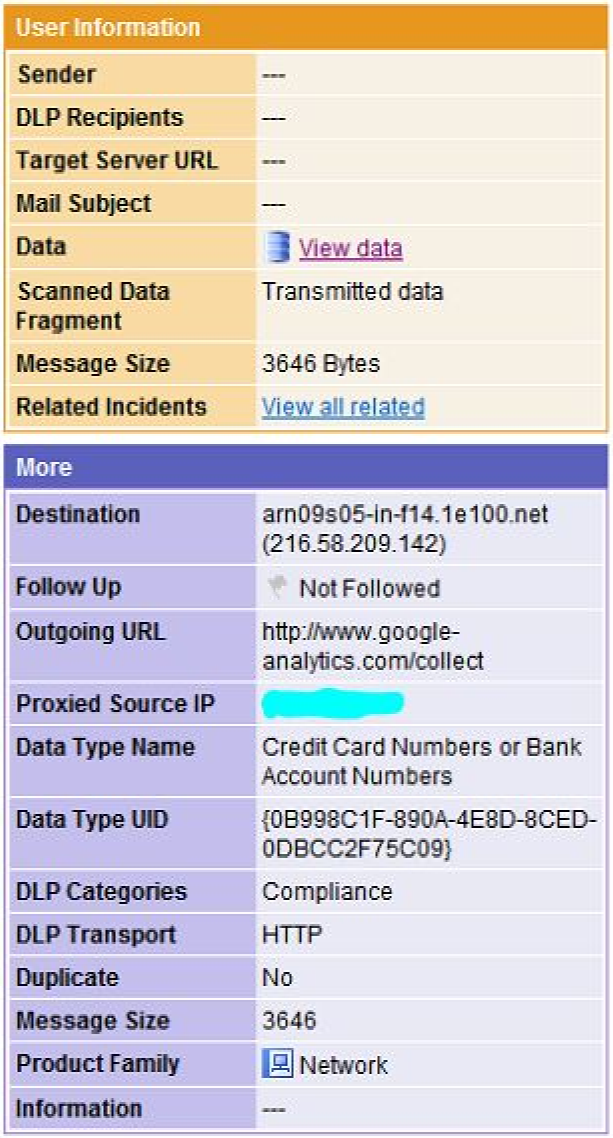
Traffic	
Source	[redacted]
Destination	arn09s05-in-f14.1e100.net (216.58.209.142)
Service	http (80)
Protocol	TCP tcp
Interface	---
Source Port	---
File Direction	tap to tap

Policy	
Policy Name	Standard
Policy Date	Fri Apr 24 18:40:38 2015
Policy Management	[redacted]

DLP Type	
Action	Detect
DLP Additional Action	---
DLP Action Reason	Rule Base
DLP Rule Name	Bank Account Numbers or Credit Card Numbers or Bank Account Numbers or Credit Card Numbers or IBAN or EU Data Protection Directive or FERPA - Confidential Educational Records or GLBA - Personal Financial Information or HIPAA - Medical Record Number - MRN or HIPAA - Protected Health Information or ITAR - International Traffic in Arms Regulations or PCI - Cardholder Data or PCI - Credit Card Numbers or PCI - Credit Card Numbers - 20 or more or PCI - Credit Card Numbers - 5 or more or PCI - Magnetic Stripe Data or PCI - Sensitive Authentication Data
Message to User	You have sent a message which ... More
DLP Words List	23980787, 23982232, 15547648, ... More
DLP Watermark Profile	---
DLP Relevant Data Types	Bank Account Numbers
Severity	Medium

Figure 6: Detailed information on data transferred in session

It also shows information of the user that has sent this information. In normal operations this will be placed on the internal network with connections to some LDAP source like Microsoft Active Directory which will gather both username, computername and related information.

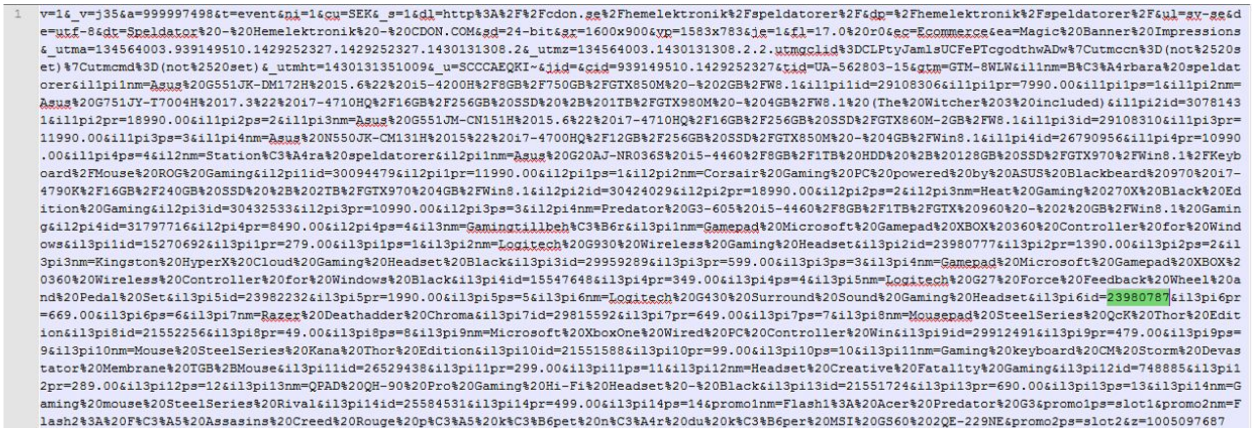


User Information	
Sender	---
DLP Recipients	---
Target Server URL	---
Mail Subject	---
Data	View data
Scanned Data Fragment	Transmitted data
Message Size	3646 Bytes
Related Incidents	View all related

More	
Destination	arn09s05-in-f14.1e100.net (216.58.209.142)
Follow Up	Not Followed
Outgoing URL	http://www.google-analytics.com/collect
Proxied Source IP	[redacted]
Data Type Name	Credit Card Numbers or Bank Account Numbers
Data Type UID	{0B998C1F-890A-4E8D-8CED-0DBCC2F75C09}
DLP Categories	Compliance
DLP Transport	HTTP
Duplicate	No
Message Size	3646
Product Family	Network
Information	---

Figure 7: Example of detailed information about user and data

When it discovers a data leakage incident it will register the data that is transmitted or do a packet capture if you like that kind of information. You can then have a look at the data, if it is an email it will open up a copy of the email that was sent.



```
v=1&_v=j35&a=999997498&t=event&ni=1&cu=SEK&_s=1&dl=http%3A%2F%2Fcdon.se%2Fhemelektronik%2Fspeldatorer%2F&dp=%2Fhemelektronik%2Fspeldatorer%2F&ul=sv-se&d
e=utf-8&dt=Speldator%20-%20Hemelektronik%20-%20CDON.COM&sd=24-bit&sr=1600x900&vp=1583x783&je=1&fl=17.0%20r0&ec=Ecommerce&ea=Magic%20Banner%20Impressions
&_utma=134564003.939149510.1429252327.1429252327.1430131308.2&_utmz=134564003.1430131308.2.2.utmgclid%3DCLPtyJamlsUCFePTcgodthwADw%7Cutmccn%3D(not%2520s
et)%7Cutmcmd%3D(not%2520set)&_utmht=1430131351009&_u=SCCCAEQKI~&jid=&cid=939149510.1429252327&tid=UA-562803-15&gtm=GTM-8WLW&il1nm=B%C3%A4rbara%20speldat
orer&il1pi1nm=Asus%20G551JK-DM172H%2015.6%22%20i5-4200H%2F8GB%2F750GB%2FGTX850M%20-%202GB%2FW8.1&il1pi1id=29108306&il1pi1pr=7990.00&il1pi1ps=1&il1pi2nm=
Asus%20G751JY-T7004H%2017.3%22%20i7-4710HQ%2F16GB%2F256GB%20SSD%20%2B%201TB%2FGTX980M%20-%204GB%2FW8.1%20(The%20Witcher%203%20included)&il1pi2id=3078143
1&il1pi2pr=18990.00&il1pi2ps=2&il1pi3nm=Asus%20G551JM-CN151H%2015.6%22%20i7-4710HQ%2F16GB%2F256GB%20SSD%2FGTX860M-2GB%2FW8.1&il1pi3id=29108310&il1pi3pr=
11990.00&il1pi3ps=3&il1pi4nm=Asus%20N550JK-CM131H%2015%22%20i7-4700HQ%2F12GB%2F256GB%20SSD%2FGTX850M%20-%204GB%2FWin8.1&il1pi4id=26790956&il1pi4pr=10990
.00&il1pi4ps=4&il2nm=Station%C3%A4ra%20speldatorer&il2pi1nm=Asus%20G20AJ-NR036S%20i5-4460%2F8GB%2F1TB%20HDD%20%2B%20128GB%20SSD%2FGTX970%2FWin8.1%2FKeyb
oard%2FMouse%20ROG%20Gaming&il2pi1id=30094479&il2pi1pr=11990.00&il2pi1ps=1&il2pi2nm=Corsair%20Gaming%20PC%20powered%20by%20ASUS%20Blackbeard%20970%20i7-
4790K%2F16GB%2F240GB%20SSD%20%2B%202TB%2FGTX970%204GB%2FWin8.1&il2pi2id=30424029&il2pi2pr=18990.00&il2pi2ps=2&il2pi3nm=Heat%20Gaming%20270X%20Black%20Ed
ition%20Gaming&il2pi3id=30432533&il2pi3pr=10990.00&il2pi3ps=3&il2pi4nm=Predator%20G3-605%20i5-4460%2F8GB%2F1TB%2FGTX%20960%20-%202%20GB%2FWin8.1%20Gamin
g&il2pi4id=31797716&il2pi4pr=8490.00&il2pi4ps=4&il3nm=Gamingtillbeh%C3%B6r&il3pi1nm=Gamepad%20Microsoft%20Gamepad%20XBOX%20360%20Controller%20for%20Wind
ows&il3pi1id=15270692&il3pi1pr=279.00&il3pi1ps=1&il3pi2nm=Logitech%20G930%20Wireless%20Gaming%20Headset&il3pi2id=23980777&il3pi2pr=1390.00&il3pi2ps=2&il
3pi3nm=Kingston%20HyperX%20Cloud%20Gaming%20Headset%20Black&il3pi3id=29959289&il3pi3pr=599.00&il3pi3ps=3&il3pi4nm=Gamepad%20Microsoft%20Gamepad%20XBOX%2
0360%20Wireless%20Controller%20for%20Windows%20Black&il3pi4id=15547648&il3pi4pr=349.00&il3pi4ps=4&il3pi5nm=Logitech%20G27%20Force%20Feedback%20Wheel%20a
nd%20Pedal%20Set&il3pi5id=23982232&il3pi5pr=1990.00&il3pi5ps=5&il3pi6nm=Logitech%20G430%20Surround%20Sound%20Gaming%20Headset&il3pi6id=23980787&il3pi6pr
=669.00&il3pi6ps=6&il3pi7nm=Razer%20Deathadder%20Chroma&il3pi7id=29815592&il3pi7pr=649.00&il3pi7ps=7&il3pi8nm=Mousepad%20SteelSeries%20QcK%20Thor%20Edit
ion&il3pi8id=21552256&il3pi8pr=49.00&il3pi8ps=8&il3pi9nm=Microsoft%20XboxOne%20Wired%20PC%20Controller%20Win&il3pi9id=29912491&il3pi9pr=479.00&il3pi9ps=
9&il3pi10nm=Mouse%20SteelSeries%20Kana%20Thor%20Edition&il3pi10id=21551588&il3pi10pr=99.00&il3pi10ps=10&il3pi11nm=Gaming%20keyboard%20CM%20Storm%20Devas
tator%20Membrane%20TGB%2BMouse&il3pi11id=26529438&il3pi11pr=299.00&il3pi11ps=11&il3pi12nm=Headset%20Creative%20Fatal1ty%20Gaming&il3pi12id=748885&il3pi1
2pr=289.00&il3pi12ps=12&il3pi13nm=QPAD%20QH-90%20Pro%20Gaming%20Hi-Fi%20Headset%20-%20Black&il3pi13id=21551724&il3pi13pr=690.00&il3pi13ps=13&il3pi14nm=G
aming%20mouse%20SteelSeries%20Rival&il3pi14id=25584531&il3pi14pr=499.00&il3pi14ps=14&promo1nm=Flash1%3A%20Acer%20Predator%20G3&promo1ps=slot1&promo2nm=F
lash2%3A%20F%C3%A5%20Assasins%20Creed%20Rouge%20p%C3%A5%20k%C3%B6pet%20n%C3%A4r%20du%20k%C3%B6per%20MSI%20GS60%202QE-229NE&promo2ps=slot2&z=1005097687
```

Figure 8: Example of raw data collected by DLP

5.2 Interviews

The meetings with the participant companies started with an interview to get to know them better and to create a baseline on what to search for during the traffic data collection. Here is the list of questions that was asked during the interviews and why we asked just those questions.

1. ***How many work with Information Security?***

According to the ISO 27002 there should be a information security organization. We wanted to know if the organizations had such a organization and how many that were involved.

2. ***Who is responsible for the ISSP?***

Certain roles has to be filled according to the ISO 27002 regarding what the ISSP has to include. We wanted to know if the policy fulfills those ISO requirements and whether or not the interview answer reflects their ISSP.

3. ***How is the ISSP updated?***

There can be several reasons as to why the individuals are not compliant with the ISSP which is why the ISSP should be updated and reflect current practices (Kolkowska & Dhillon, 2013). SETA states that the individuals should be aware of the ISSP existence and the current versions. According to the ISO27002 a ISSP should exist within the organization and that it should be updated regularly to keep up with current threats and vulnerabilities. We wanted to know if such a ISSP existed and how regular it was updated.

4. ***How do you distribute knowledge of the ISSP?***

The individuals within the organization should always be aware of the current version of the ISSP in order to avoid risk and vulnerabilities (Bulgurcu et al, 2010; D'Arcy et al, 2009). We wanted to know how the individuals were notified about the updates and whether or not the individuals were aware of the current version and security procedures.

5. ***How are the users aware of the risks associated with data leakage?***

Individuals have a tendency to be insufficiently informed about the security risks and threats around them (Adams & Sasse, 1999; Bulgurcu et al, 2010). Several researchers have speculated the need to educate and train the individuals about the threats and how to handle them (Dhillon 1999, Parker 1998, Whitman 2004). We wanted to know if this process was implemented.

6. ***How do you educate the users in risk mitigation?***

According to Bulgurcu et al (2010) there are several ways for a individual to be educated about the risks such as personal experience of attacks and complyances with security rules and regulations, newspaper, journals etc.Bulgurcu et al (2010) and D'Arcy et al (2009) believes that there is a need for SETA to educate the individuals on how to mitigiate security risks. We wanted to know if the users got security education on how to act securely and if they were presented with the strategy from the IT department.

7. ***Which compliance regulations are the organization bound to follow?***

Webspy (2009) states that there are two types of data which the organizations need to protect in order to prevent data leakages, regulatory compliance which is e.g. private information or personally-identifiable information, and intellectual property protection which is the organization’s assets, confidential data etc. We wanted to know if the organization followed any compliance regulations, to be able to create trigger to the firewalls based on this type of data.

8. ***Are you aware of any breaches that has happened?***

With knowledge of how the security procedure works its possible for malicious individuals to erase the evidence after himself, the organization might therefore never know that a security breach has occurred (Ahmad et al, 2013; Blasco et al, 2012; Chivers et al, 2009; Colwill, 2009, Moore et al, 2009; Walker ,2008)**.** We wanted to know if they were aware of any breaches, how they handled those and how they were made aware of the breach.

9. ***What would the impact of knowledge leakage be?***

Knowledge has a monetary value. The impact of knowledge leakage has a direct cost but even an indirect cost as loss of reputation (Ahmad et al, 2013; Blasco et al, 2012; Colwill, 2009). We asked this question to see if the companies have performed a risk assessment and valued their intellectual assets.

10. ***What kind of data do you consider sensitive and should not leave the company premises?***

Different companies have different kind of data that is considered sensitive. A software development company would say their source code, a bank would mention their financial transactions. We asked this question to see if they had given this topic a thought, and to be able to focus the event triggers so that the firewall could register the incidents of data leakage based on the data provided with this question.

11. ***How are you made aware if someone leaks data?***

According to Bulgurcu et al (2010) and D’Arcy et al (2009) monitoring is a needed security countermeasure meant to reduce information security misuses, intentions to misuse and unintentional accidents by the individuals. We asked this question to see if the companies had some kind of data leakage detection in place, or if it was just based on someone reporting a leakage.

12. What actions do you take to improve the security culture?

SETA is meant to educate the individuals what to look out for, how to handle it and still be compliant with the ISSP (Bulgurcu et al, 2010; D'Arcy et al, 2009). ISSP, SETA and monitoring are some security countermeasures against security breaches (Ibid). DLP is a technical solution supposed to prevent data leakage (Blasco et al, 2012). We asked this question to get to know if security awareness was prioritized in the companies.

13. How do you handle insider breaches?

According to Chen, Ramamurthy, & Wen (2012) individuals more less prone to perform security breaches if they know that they are being monitored and will be punished for such action. Also, by giving reward to those who act/perform in a positive way are more likely to avoid and even help prevent security breaches. We wanted to know what kind of approach the companies focused on.

5.2.1 Case 1

Case 1 was performed in a Swedish municipality. The municipalities are very open and free organizations, and most of what they are doing isn't sensitive. On the other hand, what is sensitive is very sensitive. They are handling cases through social services, immigrations and health care.

This specific municipality is of a medium size in Swedish terms with approximately 25000 residents and they employ somewhere around 2000 people.

We started the interview with the question *How many works with Information Security*.

The answer to that question was quite fuzzy. They have a distributed set of working with information security, where everyone is responsible for their own actions and have to make sure they are handling sensitive information the right way. On a more specific area, they don't have anyone working with Information Security to make sure it is handled the right way. The take a common responsibility.

The next question was *Who is responsible for the ISSP?* Even that was a question with a fuzzy answer. The ISSP is created within the organization, but is given to the city council to approve or reject it. When it is approved, the organization has to follow it until there is a new ISSP available. The organization can not decide on a policy itself, the policy needs to go through the city council. The organization can though create guidelines.

Question number three was *How is the ISSP updated?* In the municipality there isn't a defined process or a lifecycle on updating the ISSP. Due to the amount of different services within the municipality they have many different needs to take into considerations. So the general rule is that everything that is work related is allowed. The ISSP states what is most important to keep secured, and hence it is updated when "someone" sees the need to update it due to changes to the environment.

The next question was *How do you distribute knowledge of the ISSP?* In this company the ISSP is signed when you get hired. The employee are self responsible to find and go through the updated ISSP's which is published on the Intranet and is available to all employees. The Intranet consists of a feature which shows the user which documents are recently updated.

Going further we asked the question *How are the users made aware of the risks associated with data leakage?* The organization does not have security awareness training, so this is based on common sense and that users are raising questions to the IT Helpdesk or some superior on this topic.

Following that we asked the question *How do you educate the users in risk mitigation?* As mentioned in the last question, there is no security awareness training within the organization. So even here the organization base the security measures on the clients using common sense. Today users know they shouldn’t click on a link in an email if they don’t know who it is from, and that they should not give away their password to anyone else.

We then moved over to a section on previous breaches starting with the question *Which compliance regulations are the organization bound to follow?* Since it is a municipality it has to follow the laws and regulations for such organizations. Examples of this is Arkivlagen and Personuppgiftslagen which handles respectively archives in public sector and handling personally identifiable information.

We then asked the question *Are you aware of any breaches that has happened?* They told that they didn’t know of any data leakages that has happened, but they had been victims for DDoS attacks and larger outages. They did mention that even though they didn’t know of any data leakage incidents that they were quite sure some of those had taken place, but didn’t have the tools to neither prevent nor detect such breaches.

The next question was *What would the impact of knowledge leakage be?* The impact for a municipality is quite different than the one of a private company. As an example, an incident where sensitive data is leaked will not make someone move to another municipality. Of course it would lead to a bad reputation. For a municipality it might also lead to investigations and fines.

After that we moved to the question *What kind of data do you consider sensitive, and should not leave the company premises?* One of the reasons for this question is to make a baseline on what data leakage events should trigger an alarm for the data collection part of the thesis work. The most frequent sensitive data is personally identifiable information. They do have information about all residents and uses PII in their daily work, but this should not be leaked outside the municipality. Data from social security is in general sensitive, the same goes for healthcare information. For those we decided to work with HIPAA.

The next question was *How are you made aware if someone leaks data?* The organization does not have any tools that can detect data leakage, so being proactive is not possible. The only way of being made aware of data leakage is if someone else tell them it has happened. This has never happened to the municipality at the time of the interview.

Going further we asked the question *What actions do you take to improve the security culture?* Working on the security culture was a task they had been talking about, but due to time constraints that had not been prioritized. They do though work on general culture and being respectful and humble in contact with each other and external parties, and hopefully that will also help on the security culture.

The last question we asked was *How do you handle insider breaches?* If they are made aware of a user that has leaked data this user will be handed a written reprimand. If this repeats it might lead to disciplinary actions or even legal actions.

5.2.2 Case 2

Case 2 was performed within an international software developer company with offices all through Europe. The company has a huge market share within their niche and needs to protect both the intellectual property as well as information on customers and product roadmap.

We started the interview with the question *How many works with Information Security*. The organization does not contain someone that works with Information Security exclusively, but a couple of people have Information Security as part of their job description. Their task is to create ISSP and to secure that their product is hardened to a necessary level.

The next question was *Who is responsible for the ISSP?* The IS/IT Manager is responsible that the organization has an ISSP, but the task of creating one and updating it throughout the lifecycle is distributed.

Question number 3 was *How is the ISSP updated?* In the company the ISSP is updated in an ad-hoc fashion whenever someone realizes the ISSP does not cover some elements or if a case come up and a walkthrough shows that it isn't sufficient to handle the actual environment. If the ISSP should be updated it is done with one person as project manager and performed in workshops. There is no defined lifecycle for the ISSP.

The next question was *How do you distribute knowledge of the ISSP?* During the onboarding process new employees go through an introduction program that is consisting of among other the ISSP. Of course the new employees have to sign the ISSP upon getting IT tools made available to them. The ISSP is made available to the users through the document management tool. An issue with that is that external consultants do not have access to the document management system. If a new version is created there will be information about this on the corporate Intranet.

Going further we asked the question *How are the users made aware of the risks associated with data leakage?* This is also performed during the onboarding process. There is no security awareness training implemented at this point due to time constraints, so there is no follow-up on the information given through the onboarding. A first draft of a security awareness training has been made.

Following that we asked the question *How do you educate the users in risk mitigation?* This is also covered verbally in the onboarding process. Educating users is also a part of the procedure if the service desk is receiving a case where the end user obviously is lacking knowledge. Other than that the company is relying on common sense, most of the users are highly educated within IT.

We then moved over to a section on previous breaches starting with the question *Which compliance regulations are the organization bound to follow?* This company does not have any compliance regulations that they have to follow.

We then asked the question *Are you aware of any breaches that has happened?* This question brought up a couple of critical incidents, but those are of DDoS attacks and outages. To the company's knowledge there has not been any data leakage incidents.

The next question was *What would the impact of knowledge leakage be?* This has been covered in the risk assessment the company has performed, and the impact stated there would be reduced confidence in the market, based on the severity it could even lead to loss of customers or fines.

After that we moved to the question *What kind of data do you consider sensitive, and should not leave the company premises?* One of the reasons for this question is to make a baseline on what data leakage events should trigger an alarm for the data collection part of the thesis work. The company works tightly with their customers, and hence customer information is sensitive. They make a living of developing software, so the source code is important to keep secured, mostly based on the loss of reputation if it is lost.

The next question was *How are you made aware if someone leaks data?* As of today there is no system implemented to detect data leakage. Due to that it is not possible for the company to be proactive, the only way to be made aware is either by coincidence that it is revealed while looking for something else or that someone else tells the company data has been leaked.

Going further we asked the question *What actions do you take to improve the security culture?* This is also worked on during the onboarding process. The onboarding process consists of a one-on-one walkthrough which also covers security policy and practices. During that walkthrough the users get an introduction to the security procedures. If everyone follows those procedures there will be a good security culture. After the onboarding process the company servicedesk use opportunities to educate users, in a respectful way. You can not create a culture with force.

The last question we asked was *How do you handle insider breaches?* If an incident is reported that an insider has leaked data this will be a case for HR. Depending on the severity of the breach an oral or a written reprimand is given to the user. If the same person performs more breaches they might be even be fired.

5.3 Information system security policy

5.3.1 Case 1

Company 1, the municipality, has a very open policy where nothing is unacceptable. The government should in general not perform censorship, and that is the line that company 1 is following too.

The general rule is that everything a user does is traceable and could be reviewed, so ethics and moral is important. The main reason for the policy is to limit disturbance in the IT systems, so that everyone can use the systems to perform the tasks they should.
The policy states that the IT systems is only to be used for work related tasks, and that the employee should keep accounts and passwords secret.

Going forward the policy also mentions that the employee has to act in a way that can prevent sabotage or disturbances to other users and central systems. One way of approaching that is that users are not allowed to connect equipment that is not managed by the IT department to the network.

Copying or distribution of copyrighted material is not allowed unless the data owner has approved to that, and distribution of material in general can be limited if necessary due to financial reasons.

Furthermore the policy states that the IT department stores logs of all traffic for three months so they can handle daily operations or troubleshoot incidents, as well as monitor suspected security breaches. They also have the right to disable access due to security breaches and have obligation to report that to the employee's manager that makes the decision on how to handle the breach.

The policy also states that the social security department and the IT department are obligated to implement access control to information that is covered by the swedish law for patient information (Patientdatalagen).

The Non-Disclosure Agreement that is used with social security and education services states that personally identifiable information should not be revealed unless the person or his relatives are not harmed by the information and accepts this. Finally it states that the NDA covers parts of the areas handled by social security and education services.

5.3.2 Case 2

Company 2 is a private company and has developed several different policy documents that in total creates their Information System Security suite.

The first one is a user account policy that states that accounts are personal and that you should keep it secure by using a 12 letter password that is hard to guess and is kept private. It also states that a user should never share their password, and if they suspect someone has gotten ahold of their password the user should change their password immediately. They should even not make a note of their password in an unsecure way nor store it in a way so other can understand it is a password.

The next one shared with us is the PC policy which consists of regulations on what can be installed on the computer, that copyrighted material should not be stored on the computer and that personal equipment should not be connected to the company internal network. It is worth to mention that they have a separate physical network where users can connect other equipment, and that a 802.1x network is under implementation to improve security on just that point. The policy also states that users are not allowed to implement technical solutions that can jeopardize the corporate security, at least not without acceptance from the IT department. The policy even states that visiting websites with illegal, obscene or offensive material is prohibited.

Some users are granted local administrator rights on their computers, and they have a separate policy that has to be followed for those users. This policy states that installation of copyrighted software without a company handled serial number is not allowed, as well as installing of software that is not work-related. Disabling or making changes to running antivirus client is also specified as prohibited as well as changing components of the preinstalled Windows image.

The final policy we got ahold of is the main Information System Security Policy. This policy starts with declaring the security organization of the company. There is no dedicated responsible person for security questions, but rather a group of people that is mentioned with the IT Manager as utterly responsible. On a side note this organizational view is deprecated as new people have the roles that is mentioned in the policy.

The policy itself starts with stating the main principles. The main principle is that security is based on the potential damage an incident can result in. Further it states that all incidents have to be reported, they have to follow rules and regulations and that all systems have to have a defined owner which is responsible to have security features implemented, used and audited. Following that the basic rules state that all equipment is meant for work-related tasks, all devices have to have the latest security patches installed and have to be approved by the IT department prior to connection to the network.

Going further there is a chapter on user accounts. Based on the information in the user account policy, which is referred to in the ISSP, this seems quite redundant. But some points are different, like that user accounts not being used for 6 months will be disabled, and 6 months after that they will be deleted. This chapter also contains a bullet point on reproduction of data to lists, memory sticks, CD ROM or laptop storage is prohibited. Here it states that data leakage is not allowed!

After that they state in a subchapter that the IT Department distributes a password protected screensaver that must not be changed, and every time you leave your computer you have to lock the running session. At the end of the day you should power off the computer.

In the next chapter they state what information is prohibited for storing on network connected storage. What data is prohibited is obscene and offensive material, copyrighted software without a valid license, copyright protected material like music and videos, non work-related videos, games and finally private files like photos and such. They do not state anything on how to handle sensitive information though.

The following chapter focuses on viruses and how to prevent these, as well as how not to use email in regards to rumours, chain letters and such. They also state how to react if you suspect a virus infection. These guidelines include disconnecting the computer from the network to limit spreading of the virus as well as contacting the IT support helpdesk. The next chapters covers different types of behaviour. The first is stating what content to prevent on the Internet. Again it states the importance of not installing company supplied software, and preventing virus infected downloads. The next section is on e-mail, stating it is not allowed to automatically forward all e-mail to external mailboxes like Hotmail or GMail. It also states that giving out the e-mail address on websites or participating in mailing groups is prohibited, unless it is work related.

The next chapter focuses on securing the laptop. It states that hard drive encryption is necessary if the user have sensitive information stored on the laptop. It is also important to store and carry the computer safely, and report theft immediately to the IT Support Helpdesk.

Following there is a chapter on mobile devices. It is said in the policy that storage of sensitive information on mobile devices is not allowed, and that synchronization of email is just allowed on specific devices which are approved by the IT Department.

The next chapter focuses on remote access. VPN access is granted to employees with two factor authentication, except for mail that is available through a SSL website. The company also has VPN tunnels to customers, for which AAA is used as well as limiting access only to what is needed at the customers. Password for customer systems are stored in an encrypted database with full traceability of who has accessed a password.

The policy also contains some meanings on physical security, like keeping the desk clean, not leaving documents on the printer and not leaving any sensitive information in conference rooms.

The last policy statement is concerning information classification. The company has created their own classification system. The information is classified as public, internal or confidential, while the users accessing them are classified as public, internal users, partners or customers.

Finally the policy states the consequences of not following the policy. This results in information to the user’s manager, permissions are withdrawn and an oral or written remark or warning. For more serious incidents it may lead to dismissal, resignation and notification to the police. Information theft is an example of these more serious incidents.

5.4 Traffic report

5.4.1 Case 1

The firewall we installed was running in the live environment at the municipality for 9 days. 7 of these were working days. During this time almost 2.2 TB of data was sent over to the firewall were 303532 possible data leakage events were triggered. The Data Loss Prevention system from the firewall had created these events:

Type of data sent	Number of events
PCI - Card Security Code	298619
Credit Card Numbers or Bank Account Numbers	3494
Programming language lines (Source Code), such as C, C++, C#, JAVA	541
PCI - Expiration Date	521
PCI - Encrypted PIN Block	348
Sweden Classification Terms	9
	303532 total events

Table 2: Registered events in company 1

The different events from the firewalls are divided into the different categories as shown in the table above. The category “PCI - Card Security Code” is a data type consisting of four digit numbers. So every time data has passed through the firewall where it find a four digit number it has registered an event, no matter of other circumstances. This is part of the PCI compliance best practice, but since the municipality is not handling credit cards we have discarded all these as false positive. A false positive is when an event is created based on data that is misinterpreted. A perfect example would be just this case.

To categorize data as the data type of “Credit Card Numbers or Bank Account Numbers” the firewall are searching for a sequence of numbers that can be a credit card number or a bank account number.

The category “Programming language lines (Source Code), such as C, C++, C#, JAVA” is used when the firewall finds a block of data that is matching some of the syntax of the most used programming languages.

“PCI - Expiration date” is a category that is used when paying used a credit card. When you enter your card details you have to enter the expiration date of your credit card in the format of mm/yy. So to digits of month followed by a slash and then two digits for the year. So if a credit card expires in april 2015 the expiration date will be written as 04/15. Now all data that consists of a number lower than or equal to 12 followed by a slash and two digits will be categorized to this category.

The category “PCI - Encrypted PIN block” consists of encrypted PIN codes following one of the ISO standards. All of these will present the data as four blocks of four hexadecimal digits. So an example of the data stream would be “1412 348D 665A C5A3”. Everytime the firewall see a pattern like that it will register it as the category “PCI - Encrypted PIN block”. Even this is a part of the best practices to comply to PCI DSS.

The “Sweden Classification Terms” are terms used in Swedish military and governments to perform classification of data.

Below you see a graphical representation of the distribution of values throughout the different categories.

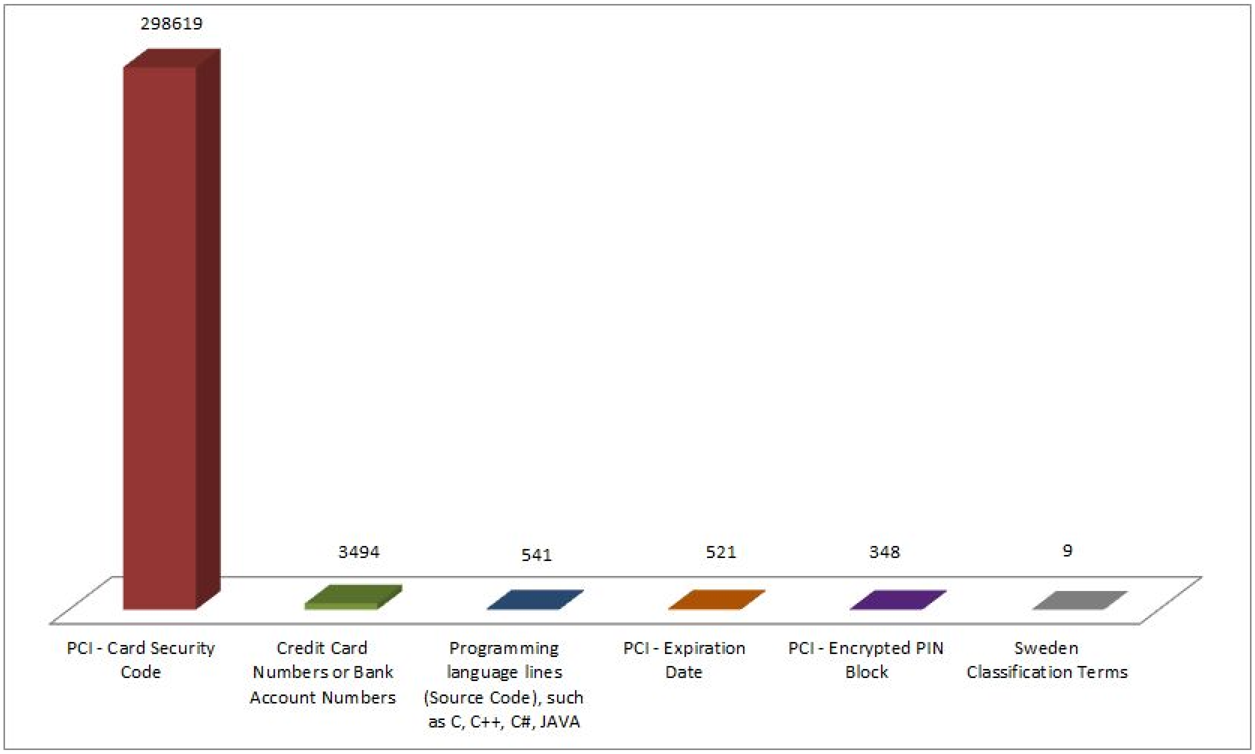


Figure 9: Graphical representation of triggered events in company 1

After analyzing all events manually we have found the following data leakage

Type of data	Number of incidents
Social Security Number, Account number, Salary	9
Social Security Number	14
List of more than 10 Social Security numbers	1
Student grades	1
Username and Password	1
Medical information	3
Social services information	3

Table 3: Events that was classified as incidents after manual inspection at company 1

So in total we found 32 breaches to the information security policy. Due to the large amount incidents reported and a limited knowledge of the company we can’t guarantee this is all. On top of that, data that is encrypted is not registered due to lack of capabilities to decrypt them for categorization. Another useful information is that all of these were sent by email.

5.4.2 Case 2

The firewall was installed at company 2 for 10 days. During these days there were only 5 ordinary working days, but the company has support for customers 24/7/365, not all the time on-site though. The company has lots of firewalls covering different parts of the business, but the only one we looked at was the perimeter firewall for Internet access. Other firewalls handled access to installations at customers, VPN tunnels to branch offices etc. During these 10 days the firewall handled 500 GigaByte of traffic. The DLP registered the following events:

Type of data sent	Number of events
Login Credentials	41
Sweden Personal Names	37
IPv4 Address - 20 or more	20
SQL Queries	13
Business Plan Terms	6
Sweden Personal Information Headers	6
Sweden Surnames	5
Sweden Names and Surnames	5
Internal Users and a New External Recipient	4
Sweden Corporate Identification Numbers	3
PCI - Cardholder Data	3
Business Plan Topics	2
Source Code - Scripts	2
External Recipient in BCC	2
Source Code - JavaScript	2

Database File	2
Active Directory or LDAP Entries	2
Source Code	2
MAC Address	2
Other	14
	185 total events

Table 4: Registered events in company 2

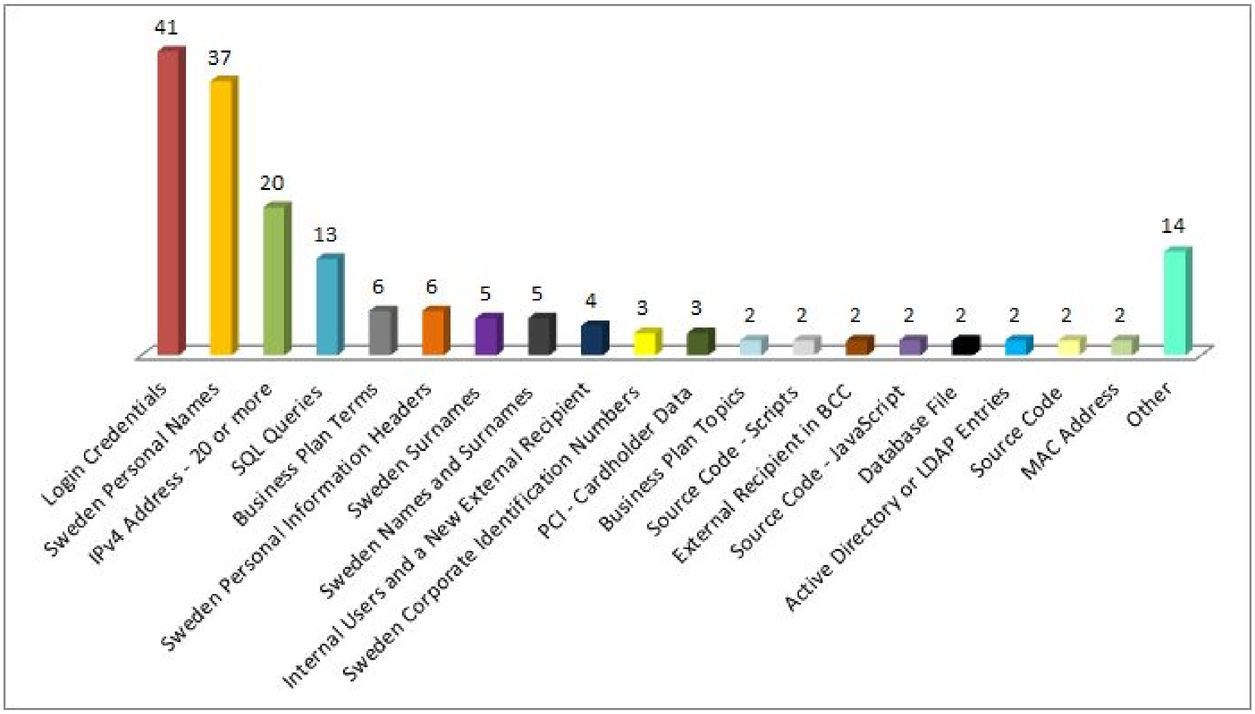


Figure 10: Graphical representation of triggered events in company 2

In the category Login Credentials the firewall looks for known ways on how to write username and password, as well as searching for the keywords username and password. This was the category where we found all the incidents at this company. We did also see external partners and customers sending login credentials into the company, but due to the fact that this was not generated within the company we did not categorize those as incidents for this specific company. You can not protect yourself from this kind of data leakage, it is really a data leakage at the sending company. One thing we did find though was that these came in through email, and response to those emails still contained the login information.

Personally identifiable information like sweden personal names, swedish names and surnames searches for data where more than 20 names from a list is found in one session. This would suggest a list of names, and could include personally identifiable information like a list of employees from HR or similar. The incidents we found here did include quite a few names, but we categorized them as false positives due to the fact that they included just names and nothing else that could identify the persons. In several cases the names was not even of employees within the company.

The category IPv4 addresses searches for numbers in a row with dots between. Most of these were not IP addresses at all, but just binary data. Some of them were IP addresses, but just IP addresses is not something that is sensitive. If it had included server names or functions it would have been different. We did not see any of these as data leakage incidents.

The company is making their revenue based on creating software with a SQL database backend. Source code and SQL queries are some of the intellectual property of the company and hence very important to protect. The ones that the DLP engine triggered was general source code that did not reveal any sensitive data so we did not categorize those either as data leakage.

After analyzing all the incidents manually we found the following data leakage incidents:

Type of data	Number of incidents
Username and Password	16

Table 5: Events that was classified as incidents after manual inspection at company 2

5.5 ISO 27002:2013

ISO 27002:2013 is a code of practice for information security controls. This is made by the ISO organization and cover a step by step guide on how to implement information security controls, and how to write a Information System Security Policy. Below is a list on the different categories mentioned in the standard, with bullet points on what to include and some information we have added on what details these bullet points should cover. This is what the ISO 27002:2013 recommends the policy should be built upon. Every item is not necessary, the standard is just a framework and needs adaption to the local reality in each company that applies the standard.

- Organization of information security
    - Internal organization
        - Roles, responsibilities, duties
    - Mobile devices and teleworking
        - Policies for mobile devices and teleworking
- Human resource security
    - Prior to employment
        - Screening
    - During employment
        - Education, training, management responsibilities
    - Termination and change of employment
        - Responsibilities
- Asset management
    - Responsibility for assets
        - Inventory, ownership, acceptable use
    - Information classification
        - Classification, labeling and handling
    - Media handling
        - Removable media handling, disposal and transfer
- Access control
    - Business requirements of access control
        - Access control and service access
    - User access management

        - User registration, de-registration, access provisioning, privileged access, audits
    - User responsibilities
        - Use of secret authentication information
    - System and application access control
        - Logon procedures, password management, access restrictions, use of privileged programs
- Cryptography
    - Cryptographic controls
        - Cryptographic policies and key management
- Physical and environmental security
    - Secure areas
        - Physical security, entry controls, loading areas, working in secure areas
    - Equipment
        - Clear desk and clear screen policies, equipment protection, cabling security etc.
- Operational security
    - Operational procedures and responsibilities
        - Change and capacity management, operating procedures
    - Protection from malware
        - Control against malware
    - Backup
        - Information backup
    - Logging and monitoring
        - Event, administrator and operator log, log protection, time sync
    - Control of operational software
        - Software installation procedures and policies
    - Technical vulnerability management
        - Vulnerability management and software restrictions
    - Information systems audit considerations
        - Audit controls
- Communications security
    - Network security management

    - Network controls, segregation and services security
  - Information transfer
    - Transfer agreements, policies and procedures and NDA
- System acquisition, development and maintenance
  - Security requirements in information systems
    - Securing transactions, application services and requirements
  - Security in development and support processes
    - Secure development, change control, release management and acceptance testing
  - Test data
    - Protection of test data
- Supplier relationship
  - Information security in supplier relationships
    - Supply chain, supplier agreements and security policy
  - Supplier service delivery management
    - Monitoring, reviewing and changes to supplier services
- Information security incident management
  - Management of information security incidents and improvements
    - Responsibilities, procedures, reporting of weaknesses and events, response on incidents and collection of evidence
- Information security aspects of business continuity management
  - Information security continuity
    - Plan, implement and review security continuity
  - Redundancies
    - Availability of services
- Compliance
  - Compliance with legal and contractual requirements
    - Identification of legislation, protecting intellectual property and personally identifiable information
  - Information security reviews
    - Independent reviews, compliance with standards and technical compliance

Chapter VI

6. Analysis

6.1 Pattern matching - Interviews & policy

6.1.1 Case 1 - Company 1

Nr	Question	Answer	Policy
1	How many work with Information Security?	No named person or role	Does not mention organization
2	Who is responsible for the ISSP?	No named person or role, city council has to approve	Does not mention responsibility
3	How is the ISSP updated?	Ad-hoc	Lifecycle or lifetime is not mentioned in the policy
4	How do you distribute knowledge of the ISSP?	During onboarding, updates distributed on the Intranet	The policy does not mention anything on how to get updates nor the user's responsibility to stay updated
5	How are the users aware of the risks associated with data leakage?	Common sense and through IT Helpdesk	Does not mention anything on security awareness programs
6	How do you educate the users in risk mitigation?	Common sense and through IT Helpdesk	Does not mention anything on security awareness programs
7	Which compliance regulations are the organization bound to follow?	Law for archiving, handling patient information and personally identifiable information	The policy does mention that the municipality has implemented access control according to the law of patient information
8	Are you aware of any breaches that has happened?	No known data leakages	Not applicable

9	What would the impact of knowledge leakage be?	Legal investigation and fines	Not applicable, should be covered in risk assessment
10	What kind of data do you consider sensitive, and should not leave the company premises?	PII and medical information	The policy states that some information from social services should remain confidential
11	How are you made aware if someone leaks data?	Word of mouth	The policy does not mention anything on reporting of incidents
12	What actions do you take to improve the security culture?	Works on general culture improvements, hopes it affects security culture too	The policy does not mention how you should act securely
13	How do you handle insider breaches?	Written reprimands, repeated incidents might result in disciplinary or legal actions	The policy does not mention effects of not following the policy

Table 6: Pattern matching of interview and policy in company 1

6.1.1.1 Findings from the comparison of interview and policy in company 1

There is one question that shows a mismatch between the policy and the interview, the part on sensitive information (question 10) differs from the interview to the policy. The policy only states that some information from social services should remain confidential, while the interview revealed that other information elements should also be preserved.

The answers through the interview shows an indication of some informal policies. Several points were made through the interviews that isn’t mentioned in the policy. The questions regarding the security organization (question 1 & 2) was vaguely answered in the interview, but was not mentioned in the policy. The same thing goes for the information on how the ISSP is updated, how knowledge of the ISSP is distributed and security awareness training (question 3-6). The questions on reporting, working on culture and handling of incidents (questions 11-13) were also pinpointed through the interview, but not mentioned in the policy.

Question 7 regarding compliance regulations are though sanctioned in the policy.

6.1.2 Case 2 - Company 2

Nr	Question	Answer	Policy
1	How many work with Information Security?	One person has a part time role of doing this	This role is not mentioned in the policy
2	Who is responsible for the ISSP?	IT Manager	Organization of decision making is defined in the policy
3	How is the ISSP updated?	AD Hoc when needed	Lifetime is not mentioned in the policy, but it is outdated
4	How do you distribute knowledge of the ISSP?	Onboarding, new versions are introduced through the Intranet. Effective version in document management system	The document ID in the document management system is stated in the policy.
5	How are the users aware of the risks associated with data leakage?	Onboarding. Security Awareness training first draft is made.	Does not mention anything on security awareness training
6	How do you educate the users in risk mitigation?	Onboarding and through helpdesk	Not mentioned in the policy
7	Which compliance regulations are the organization bound to follow?	None	Not applicable
8	Are you aware of any breaches that has happened?	No known data leakage incidents	Not applicable
9	What would the impact of knowledge leakage be?	Reduced confidence, or even loss of customers or fines.	Mentioned in the risk assessment
10	What kind of data do you consider sensitive, and should not leave the company premises?	Customer information and source code	Data classification is mentioned in the policy, but not any specific types of data

11	How are you made aware if someone leaks data?	Word of mouth	The policy does not mention how to report possible incidents
12	What actions do you take to improve the security culture?	During onboarding and through IT Helpdesk	Not mentioned in the policy
13	How do you handle insider breaches?	HR case is created. Might result in oral or written reprimand, repeating incidents might leave to firing	Contained in the policy with more details than the interview

Table 7:Pattern matching of interview and policy in company 2

6.1.2.1 Findings from the comparison of interview and policy in company 2

Through this interview there was no major difference from the interview to the policy. Some questions was answered through the interview even though the issue was not handled in the policy. This indicates some kind of informal policy or guideline.

The part on the security awareness work (question 4 - 6) is in general handled through the on boarding process. This is not mentioned in the policy. Neither the questions on reporting of incidents nor on tasks to improve the culture are mentioned in the policy.

The rest of the questions are aligned with the policy, and we salute company 2 for their work on performing a risk assessment. The policy does not reflect the findings from the risk assessment though.

6.2 Pattern matching - Traffic & policy

6.2.1 Case 1

TYPE OF DATA INCIDENT	POLICY STATEMENT

Social Security Number, Account number, Salary	Not mentioned in the policy as sensitive data
Social Security Number	Not mentioned in the policy as sensitive data
List of more than 10 Social Security numbers	Not mentioned in the policy as sensitive data
Student grades	Not mentioned in the policy as sensitive data
Username and Password	Not mentioned in the policy as sensitive data
Medical information	The policy states that part of the information from the social security is classified as sensitive
Social services information	The policy states that part of the information from the social security is classified as sensitive

Table 8:Pattern matching of data leakage incidents and policy in company 1

6.2.1.1 Findings from the comparison of registered incidents and policy in company 1

The policy from company 1 does only recognize medical and social services information as sensitive information. The interview showed that there were other types of data that is also sensitive and should not leave the company. For the 32 incidents we discovered through the traffic analysis only 6 were of the types that according to the policy were sensitive, while 26 are of types that is not mentioned in the policy. That makes more than 81 percent of the incidents of data types that is not mentioned in the policy as sensitive.

According to our conceptual framework data leakage is either intentional due to the user’s intent to comply or unintentional based on the user’s security awareness. The process they have made for transmitting data to their external HR partner has not covered how to handle sensitive data in a secure manner. As we talked to the company it seemed like a subjective norm, it is considered OK to transmit data containing social security numbers, bank account numbers and salary in the way they do. This is being handled now after we uncovered this.

Based on this we consider this as intentional data leakage.

Many of the other incidents are most likely based on lack of awareness, since it is not repetitive and just single users that has been performing these. Users are made aware that medical information and other information from social services should be kept confidential, and most of the time that is the case. These incidents seems like single employees are not thinking what impact their actions might have, and hence we consider these unintentional.

6.2.2 Case 2

TYPE OF DATA INCIDENT	POLICY STATEMENT
Username and Password	The policy mentions a lot on personal passwords, but nothing on shared accounts passwords.

Table 9:Pattern matching of data leakage incidents and policy in company 2

6.2.2.1 Findings from the comparison of registered incidents and policy in company 2

The policy from company 2 does not define any kind of data as sensitive, but leaves it up to the user to define based on the classifications mentioned in the policy. Among the classifications confidential, internal and public we should guess that username and password should remain among the first two. This was also expressed during the interview. According to our conceptual framework this could either be a subjective norm, there is really no other way of doing this transfer and hence it is considered OK to send username and password in an insecure way. Or it could be a lack of security awareness, the users does not really understand the risks of sending username and password unencrypted. So in this case we really do not know if the data leakage is intentional or unintentional. We performed the traffic analysis in an anonymous way, so we can not ask the users what their intention was.

6.3 Cross case

6.3.1 Interviews

	Company 1	Company 2	Difference
How many work with Information Security?	No named person or role	One person has a part time role of doing this	Company 2 has a role specified
Who is responsible for the ISSP?	No named person or role, city council has to approve	IT Manager	Company 2 has a responsible specified
How is the ISSP updated?	Ad-hoc	AD Hoc when needed	None
How do you distribute knowledge of the ISSP?	During onboarding, updates distributed on the Intranet	Onboarding, new versions are introduced through the Intranet. Effective version in document management system	None
How are the users aware of the risks associated with data leakage?	Common sense and through IT Helpdesk	Onboarding. Security Awareness training first draft is made.	Company 2 has plans for SETA.
How do you educate the users in risk mitigation?	Common sense and through IT Helpdesk	Onboarding and through helpdesk	None
Which compliance regulations are the organization bound to follow?	Law for archiving, handling patient information and personally identifiable information	None	Company 1 has to follow regulations
Are you aware of any breaches that has happened?	No known data leakages	No known data leakage incidents	None
What would the impact of knowledge leakage be?	Legal investigation and fines	Reduced confidence, or even loss of customers or fines.	Both could get fines, but company 2 could also lose revenue

What kind of data do you consider sensitive, and should not leave the company premises?	PII and medical information	Customer information and source code	Completely different
How are you made aware if someone leaks data?	Word of mouth	Word of mouth	None
What actions do you take to improve the security culture?	Works on general culture improvements, hopes it affects security culture too	During onboarding and through IT Helpdesk	None really
How do you handle insider breaches?	Written reprimands, repeated incidents might result in disciplinary or legal actions	HR case is created. Might result in oral or written reprimand, repeating incidents might leave to firing	In Company 2 breaches can lead to firing of staff

Table 10:Cross-case analysis of interviews between company 1 and company 2

6.3.1.1 Findings from the comparison of interview questions between company 1 and 2

We asked the same questions to both companies, so we have the possibility to compare the answers to each other. The companies are completely different, the municipality works on handling cases to improve the community while the software development company works on developing and maintaining intellectual property. We wanted to see how this was reflected in the interviews.

Starting with the security organization company 1 does not have that organization specified. Company 2 on the other hand has that covered.

Regarding the ISSP they are aligned, except that company 2 has started a process to develop a security awareness strategy. Both companies are handling security education today as a part of the onboarding process, and both handles updates of the ISSP on an ad-hoc basis.

On the question regarding the impact of data leakage company 2 has actually performed a risk assessment, so they have quite a good knowledge of the impact. Company 1 has a good insight but are also limited to fines and bad reputation.

The question on data types that are sensitive shows a big difference. Company 1 handles personally identifiable information and medical information, while company 2 handles customer information and intellectual property.

The final difference is on effect of breaches, were the minor incidents are handled similarly while in company 2 a major incident might lead to someone getting fired.

6.3.2 Policy

ISO 27002:2013 TOPIC	Company 1	Company 2
Org - Internal organization	No	Yes
Org - Mobile devices and teleworking	No	Yes
HR Sec - Prior to employment	No	No
HR Sec - During employment	No	No
HR Sec - Termination and change of employment	No	No
Assets - Responsibility for assets	No	Yes
Assets - Information classification	No	Yes
Assets - Media handling	No	No
Access - Business requirements of access control	No	No
Access - User access management	No	Yes
Access - User responsibilities	Yes	Yes
Access - System and application access control	No	No
Crypto - Cryptographic controls	No	No
Physical - Secure areas	No	No
Physical - Equipment	No	Yes
Operational - Operational procedures and responsibilities	No	No

Operational - Protection from malware	No	Yes
Operational - Backup	No	No
Operational - Logging and monitoring	Yes	No
Operational - Control of operational software	No	Yes
Operational - Technical vulnerability management	No	No
Operational - Information systems audit considerations	No	No
Comm - Network security management	No	Yes
Comm - Information transfer	Partial	No
Systems - Security requirements in information systems	No	No
Systems - Security in development and support processes	No	No
Systems - Test data	No	No
Supplier - Information security in supplier relationships	No	Yes
Supplier - Supplier service delivery management	No	No
Incidents - Management of information security incidents and improvements	No	Yes
Continuity - Information security continuity	No	No
Continuity - Redundancies	No	No
Compliance - Compliance with legal and contractual requirements	No	Yes
Compliance - Information security reviews	No	No

Table 11: Cross-case analysis of ISO 27002:2013 policy fullfillment between company 1 and company 2

6.3.2.1 Findings from the comparison of policy fullfillments between company 1 and 2

Comparing the policies from company 1 and 2 straight off does not make sense, since they are completely different companies handling completely different types of information. The policy content is not interesting for comparison, we are more interested in the structure. Both companies has created their own policy from scratch, which gives them a good flexibility, but the risk is that they have forgotten important parts of the policy. ISO 27002:2013 is a guideline on how to create an information system security policy, it is not a demand. The companies can decide for themselves if a section is inapplicable or not, but it gives an indication on what should be a part of the policy.

The first section is regarding the organization of the security work within the company. Here company 2 is fulfilling the guidelines from ISO while company 1 is not mentioning anything regarding the organization in their policy.

In the section regarding assets company 2 has covered both the parts containing the responsibilities of the assets and information classifications. Company 1 has not covered anything of this section. None of them has covered media handling.

The section regarding access has been partially covered by both companies. Company 1 has covered user responsibilities while company 2 has even covered user access management. None of the companies has covered business requirements for access nor system and application access control.

In the section regarding physical security company 2 has covered the part containing physical access to equipment but has not covered secure areas. Company 1 has not covered this section at all.

Both companies has covered parts of the section regarding operational security. Company 1 has covered logging and monitoring, while company 2 has covered malware protection and protection of operational software.

The section regarding communication security has also been partially covered by both companies. Company 2 has mentioned network security management in their policy, while company 1 has created a NDA which is one of three sub-points within the information transfer part of the section.

Company 2 has covered the information security in supplier relationships, which is one of the parts of the supplier security section. Company 1 has not mentioned supplier security at all in their policy.

The section incident security management only consist of one part, management of information security incidents and improvements. This is covered in the policy of company 2, but not in company 1.

The final section that is covered in a policy is the compliance section. Company 2 has covered the compliance with legal and contractual requirements. The information security reviews is not a part of company 2's policy. Company 1 has not covered this section at all in their policy.

The sections HR security, cryptographic controls, systems and continuity is not covered in any the policy of any of the companies.

In total the ISO 27002:2013 consists of 15 section made of a total of 34 parts. These 34 parts consists of even more sub-points. Of the 34 parts company 1 has covered 3 of them, while company 2 has covered 13 parts. None of the parts are mandatory, but both companies has expressed a concern that there are missing parts in the policy.

6.3.3 Traffic

TYPE OF DATA INCIDENT	Company 1	Company 2
Social Security Number, Account number, Salary	9	0

Social Security Number	14	0
List of more than 10 Social Security numbers	1	0
Student grades	1	0
Username and Password	1	16
Medical information	3	0
Social services information	3	0

Table 12: Cross-case analysis of data leakage incidents between company 1 and company 2

6.3.2.1 Findings from the comparison of data leakage incidents between company 1 and 2

Company 1 and company 2 are completely different, and are handling completely different types of data. The fact that the data leakage incidents differ quite a lot was not a big surprise. Company 1 has approximately 1800 active users, so that the kind of data leakage is spread on different types of data is not a surprise either. The main distribution of incidents from company 1 was though connected to HR and social security numbers.

Company 2 had incidents only of a single type of data, username and passwords was passed to external partners in an insecure way. We were quite happily surprised that intellectual property was not a part of the incidents.

Chapter VII

7.1 Discussion

Preventing data leakage is impossible, someone will always be able to bypass the hinders you put up. They might copy data to a USB stick or a CD, but then you can prevent that. They can print data, and bring out the hardcopies. Or they can take pictures of data with their smartphones. You can put up a lot of technical means to prevent all of this, even though it might be really hard to follow up on those. What makes it totally impossible to prevent it all is all the knowledge people have in their heads which you can not limit and can not prevent to be brought outside the company premises. But even though it is impossible to come to a 100% safe data handling policy you should try to get as close as possible.

The theory of planned behavior states that intentional data leakage is based on the employee's intent to comply with the ISSP. We could not find any theories on unintentional data leakage, but based our conceptual framework on the theory of planned behavior and added lack of awareness as the reason for unintentional data leakage. We based our theoretical framework on the same theory, just added other factors to the user’s behavior that results in data leakage that is not intended. Events that was done despite policy statements it was prohibited might be due to a subjective norm, and hence is classified as intentional data leakage since they are not compliant with the ISSP. On the other hand, if the action is not mentioned in the policy the user is still in compliance with the ISSP. These events were in those cases unintentional data leakage, but the users might not have used common sense due to lack of awareness.

We did not ask the users what intentions they had when performing the actions that led to an incident. So the categorization of events in intentional and unintentional data leakage is based on comparison of the data analysed to the ISSP. Keep in mind that the data leakage is still a data leakage no matter if it is intentional or unintentional. Due to the lack of user feedback after the incidents we can not declare the severity of the breach, this is really up to the companies implied.

The DLP function in the Checkpoint Firewalls we have used is a good feature which sure can help you mitigate data leakage. But it requires lots of tuning to limit the amount of false positives. It is no artificial intelligence, it just creates an event if it find a pattern. As an example we did see from the tests in company one that it created lots of false positives due to the fact that we had enabled one of the best practices from the PCI compliance, credit card pin codes. So every time it found data consisting of a four digit number it thought it was a pin code and create a DLP event. We realize now that enabling that kind of feature on all traffic is useless. But for a finance institution adding this kind of feature on a limited part of the network might be really useful.

As of today there is a database available with lots of different data types predefined. But most of these are not working on the Swedish market. You really have to create your own data types to search for and create keyword lists for different parts of the organization. In case 1 we found one incident that was of a critical severity. It was not found due to the keywords we had defined, nor due to the data types we had specified. An event was triggered due to someone sending a large file over e-mail. And then we looked through that event and realized the data in that file was actually sensitive. So it was really based on luck that it was uncovered. On the other hand, in an operations phase you would take that kind of experience and tune the filter to make it create triggers the next time it happens. You have to realize that implementing a DLP solution is not a “set and forget” task. You have to improve the keyword database all the time, making sure you uncover more and more of the data that is leaked and even keeping it up-to-date in terms of what kind of data is added to the electronic systems of the organization.

Another finding is that to protect the company you have to perform SSL inspection. In case 1 we saw that approximately 24.4 % of the traffic was general SSL traffic. On top of that there are different applications like Dropbox and facebook that utilize SSL to secure the traffic. So SSL inspection is really crucial to ensure the organization is not leaking data. Performing SSL inspection was not possible in the implementations we have tested on, since we have not installed the firewalls inline. They have just been installed in tap mode, so traffic from the outside of the existing firewall is mirrored onto the DLP firewall we installed. In inline mode you can enable SSL inspection which will decrypt the session and set up a new session to the destination. By doing that the SSL encryption is intercepted and data can be inspected. But in our opinion that is breaking one of the key points of SSL encryption, you can’t guarantee packet authenticity anymore. So there is a decision to be made, what is more important? Securing end user integrity or organization data leakage?

Another technical difficulty on the same topic is that certificate pinning has started to become more widely used, to prevent just man-in-the-middle attacks. Certificate pinning is a technology that is used to ensure that the client certificate and the server certificate is the same and the server and client are performing dual handshakes to authorize each other. By doing that you can guarantee that no one has changed the certificate in transport between the client and the server. This will limit the possibility to perform SSL inspection as it is today, since the SSL inspection technology builds on just that, terminating the SSL tunnel midway and set up to tunnels instead. The client will then get a warning saying the tunnel is not terminated at the server, but someone between is terminating it for them. An example is Dropbox which is some kind of traffic you really want to analyze with data leakage in mind. There are also client software that can be installed to act as a certificate pinning proxy, making sure you are authenticating towards the right server. New technologies are in the making to be able to perform that kind of analysis, but it is not publicly available at the time of writing this thesis.

Worth to mention is that we asked twenty different organizations to participate in this research. Their participation would serve this research with more data and a more accurate view on the reality. The outcome would also enlighten the organizations if they have data leakage, how they occur and how they stand with dealing with data leakage compared to other organizations participating in this research. Since this research are dealing with sensitive information which has to be kept confidential against other organizations and unauthorized people we were ready to sign a nondisclosure agreement and keep the organisations anonymous. In the end, only three organisations decided to participate in this research, as for the other they decided to decline the offer of participating in the research because of security concerns. Even though most of the organisations declined to participate in the study would suggest that they are concerned of data leakage and doesn't want unauthorized people to look into their network and security. But what they fail to realise is whether or not they already have a problem with data leakage. After talking with the organizations who participated in this research they explained that this research will help them a lot in order to improve their security and minimize potential data leakage in the future. They told us that they couldn't understand why most of the organizations declined the offer to identify data leakages within the organizations for free. One of the organization even asked us to perform the same tasks as in this research but on a bigger scale and also to improve their security against data leakage. This suggest that the organizations is concerned about the data leakage which is currently going on within their organization and that they want our help, which suggest that this research was performed to their expectations.

What we also found when going through the ISSP is that they are not following any standards. There are a couple of standards that can be used to create an ISSP, one of these is the ISO 27002. As we see it there is an issue with the ISO standard not being free, the companies we talked to would like to follow a standard if it could help them assure the policy included the necessary information. But even if there is a standard it will not really help them write the policy. You really need a walk-through document to help you step by step. Due to the fact that the ISO 27002 is a paid for standard the companies rather create their own policy from scratch, and as we have seen they miss some important things and make information and decision points redundant and hard to update and verify. In other projects and classes we have used the Octave Allegro to create a risk assessment, we would really like to see someone create a similar framework and workflow for creating a security policy, it will make the world a safer place.

The ISSP from Company 1 was in general a really open policy. Almost anything is allowed, as long as the employee can show that what they do are work related. And that is just how it should be. Of course the schools need to teach things that in other companies would be seen as obscene or offensive. So limiting access to data is not an option as we see it, but it is really important that the resources are used ethically and that the students are teached how to handle that kind of information. On the other hand it would not hurt to limit access to obscene, offensive and illegal information from other parts of the organization. The other thing about the policy is that is lacks instructions on how to prevent sabotage and disturbances. It doesn’t say anything on antivirus, data encryption, system services, access control nor remote workers. And then we find it kind of strange that the NDA does not cover all sensitive data in all departments, but just personally identifiable information within social security and education services.

We can surely say that the policy from Company 2 is extensive and is covering many things. One issue is that many of the items in the policy is redundant, the same information is listed several places. As of the copies we got of the policies they are all consistent, but our concern is that if you change something you will have to update the information several places. Quite a lot of the information was also outdated, referring to systems or features that was not relevant anymore. Newer systems was not mentioned at all. We also found that some details was not covered within the different chapters, like the fact that it does not say anything on not storing confidential data on cloud storage, nor does it say anything on how to secure data in processing. It is up to the user itself to classify data, as we interpreted the policy, and also it does not say anything on how to handle customer data.

7.2 Conclusion

The results of our findings show that the main reason for unintentional data leakage is that the employee is not following procedures and policies. There might be many reasons for that behaviour. It might be that the procedures is not align with the task they perform, there might be technical systems that is missing or not working properly or it might be that the user does not know how to perform the task. Based on the incidents we found in the companies we think the main reason is lack of awareness. During this thesis work we created a theoretical framework based on the theory of planned behaviour. The theory of planned behaviour suggests that self-efficacy, subjective norms and attitude are topics that lead to intentional data leakage. To cover unintentional data leakage we added the security awareness topics as reasons for unintentional data leakage. To drill down, the unintentional data leakage is performed due to lack of security training, security education and security awareness. The results of our findings is totally in line with this theory.

To take is one step further, what can we do to mitigate this data leakage. In the perfect of worlds you would have a great security culture that would mitigate this. The security culture is the key to success. But creating a security culture is hard, it takes time and you will never get all the employees to be a part of this culture. People are different and have different views on different topics. Creating this culture consists much of doing security education, training and awareness, but is not limited to just those. You even need to make sure that the management is going in with a good example, you need to make security a part of the everyday life and make everyone think "security first". So if that perfect security culture is not there, doing a technical enforcement of the security policy is the best option.

Another thing is that most companies today have no visibility of the data that is leaving the company premises. You can not protect what you do not know about. This could be solved by installing a Data Leakage Detection mechanism. This will be less intrusive, since it will not prevent anything and you will get a good view on where you need to focus your resources.

Implementing a data leakage protection solution is not as easy as it sounds. There is really a lot of tweaking necessary to make it detect what you need. If you get to many false positives it will be hard to pinpoint what is a real incident. We saw that during company 1, since we added to the DLP that it should search for PCI compliance and hence search for PIN number we got almost 300.000 false positives. Finding the 32 real incidents was like searching for a needle in a haystack. We also found a few incidents based on pure luck. The DLP did not include any keywords for the incidents, but on the other hand it did trigger an event due to transfer of large files. So tuning the keywords is key for having a working DLP solution, and that has to be an ongoing task. Implementing a security solution must not be a set-and-forget task.

This leads us to the input for configuring the DLP solution. If we had focused just on enforcing the ISSP in these companies we would not have had many incidents. The reason for that was that the ISSP was lacking a lot of information. Based on the ISSP's shared with us we can say that it does not cover everything that should have been covered. Our suggestion is to base the ISSP on some standard, in this thesis we have compared the ISSP with ISO

27002:2013 which gives you a good baseline when creating the policy. The companies that participated in the research has created their own policies from scratch, and that is the case in many companies today. The risk is that you might miss something resulting in a policy that does not cover all necessary areas. Another thing we found was that the policies was outdated. We will therefore suggest implementing a procedure for security policy and awareness lifecycle management.

7.3 Future Research on DLP

Looking back on this research and there are a few recommendations for a new future research. One of the limitations of this thesis is the amount of organizations which participated. Most organizations where concerned of a third party looking into their security and finding flues which could be exploited. Because of the time limitation there wasn’t enough time to ask a lot of organizations to participate and have the time to collect the necessary data. As a future research it is recommended to redo this research with a larger group in order to validate the generalization of a larger population.

During the data collecting phase of the research there was a concern regarding what keywords the DLP should search for. A few keywords already existed but most of them wasn’t adapted for Swedish words or structures, which resulted in a lot of false positive findings. Therefore it is recommended to develop a database of keywords which DLP’s can utilize and raise the security level of the organizations.

Another topic is data classification, which is not much used within private organizations in Sweden as of today. The DLP solution can base rules on what template a document has been written in. So if we create different types of templates for different kind of data, as an example we can create word and powerpoint templates that should contain the different classification levels. These levels could be public information, internal and sensitive. When the employee creates a new document they should specify the template according to what type of data it contains. The metadata that is stored with the document from the template will be used for comparison, and as an example if someone is trying to send externally a document that is created with the sensitive data template it is automatically blocked. To make this work someone should create a code of practice on how to do this, and that is the part we think is lacking and could be a future research to develop.

Chapter VIII

8. References

Adams, A. & Sasse, M. (1999). *Users are not the enemy*. Communication of the ACM. December 1999/Vol. 42, No. 12

Ahmad, A., Bosua, R., & Scheepers, R. (2014). *Protecting organizational competitive advantage: A knowledge leakage perspective*. Computers & Security, 42, 27–39.

Ajzen, I. (1991). *The theory of planned behavior*. Organizational Behavior and Human Decision Processes 1991;50(2):179-211

Annansingh, F. (2005). *Exploring the risks of knowledge leakage: an information systems case study approach*. InTech Open Science, Open Minds, Croatia. [Online] http://cdn.intechopen.com/pdfs-wm/33417.pdf

Bandura, A. (1997). *Self-efficacy: toward a unifying theory of behavioral change*. Psychological Review 1977;84(2):191-215.

Bandura, A. (1991). *Social cognitive theory of self-regulation*. Organizational Behavior and Human Decision Processes 1991; 50:248-87.

Baxter, P. & Jack, S. (2008). *Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers.* The Qualitative Report Volume 13 Number 4 December 2008 544-559. [Online] http://www.nova.edu/ssss/QR/QR13-4/baxter.pdf

Bellinger, G., Castro, D. & Mills, A. (2004). *Data, information, knowledge, and wisdom*. [Online] http://geoffreyanderson.net/capstone/export/37/trunk/research/ackoffDiscussion.pdf

Blasco, J., Hernandez-Castro, C., Tapiador, E. & Ribagorda, A. (2012). *Bypassing information leakage protection with trusted applications*. Computers & Security, 31(4), 557-568.

Brendan, O. (2014). *Whoops! how your “convenience” broadcast your secrets*. American Bar Association, Chicago, United States.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). *Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness*.MIS Quarterly 2010;34(3):523-48

Chen, Y., Ramamurthy, K. & Wen, W. (2012). *Organizations’ Information Security Policy Compliance: Stick or Carrot Approach?* Journal of Management Information Systems, 29(3), 157–188.

Colwill, C. (2009). *Human factors in information security: The insider threat – Who can you trust these days?* Information Security Technical Report, 14(4), 186–196.

Creswell, J. (2013). *Research Design: qualitative, Quantitative and Mixed method Approach , 4th Edition*. SAGE Publications, Inc.

Databreaches. (2014). *Two Iowa Dept. of Human Services employees blamed for security breaches of more than 2,000 Iowans' personal information*.
[Online]
http://www.databreaches.net/two-iowa-dept-of-human-services-employees-blamed-for-security-breaches-of-more-than-2000-iowans-personal-information/

D'Arcy, J., Hovav, A. & Galletta, D. (2009). *User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach*. Information Systems Research, 20(1), 79–98.

ECS. (2014). *DLP Key Features.* [Online]
http://ecs.arrow.com/suppliers/documents/RSASolutionBrief-enVisionSolutions.pdf

Grant, I. (2009). *Insiders cause most IT security breaches, study reveals*.
[Online]
http://www.computerweekly.com/news/1280090551/Insiders-cause-most-IT-security-breaches-study-reveals

Goel, S., & Shawky, H. (2009). *Estimating the market impact of security breach announcements on firm values.* Information and Management, 46, 404–410.

Herath, T. & Rao, R. (2009). *Protection motivation and deterrence: a framework for security policy compliance in organizations.* European Journal of Information Systems 2009;18(2):106-25.

Herath, Y. & Kozar, A. (2005). *Investigating factors affecting the adoption of anti-spyware systems.* Communications of the ACM 2005; 48(8):72-7.

Inside Housing (2012). *Landlord in hot water over accidental data breach*. [Online]
http://www.insidehousing.co.uk/landlord-in-hot-water-over-accidental-data-breach/6524250.article

Kanagasingham, P. (2008). Data Loss Prevention. SANS Institute InfoSec Reading Room.
[Online] http://www.scribd.com/doc/81383468/Data-Loss-Prevention-32883#scribd

Kaspersky. (2014). *Kaspersky Lab Survey Identifies Internal IT Threats in Businesses and Infrastructure that Lead to the Most Data Loss.* [online]
http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-Survey-Identifies-Internal-IT-Threats-in-Businesses-and-Infrastructure-that-Lead-to-the-Most-Data-Loss

Kavanagh, J. (2006). *Security special report: the internal threat*. Computer Weekly, 25/4/06.

[Online]
http://www.computerweekly.com/Articles/2006/04/25/215621/security-special-report-the-internal-threat.htm

Knapp, J. & Ferrante, J. (2012). *Policy Awareness , Enforcement and Maintenance : Critical to Information Security Effectiveness in Organizations*. Journal of Management Policy and Practice vol.13(5)

Kolkowska, E. & Dhillon, G. (2013). *Organizational power and information security rule compliance*. Computers & Security, vol 33, p3–11.

Lapke, M. (2006). *A Semantic Analysis of Security Policy Formulation and Implementation : A Case Study Formulation and Implementation : A Case Study*. AMCIS, Association for Information Systems, pg 166.

Lee, Y. & Larsen, R. (2009). *Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software*. European Journal of Information Systems 2009;18(2): 177-87.

Leonard, LNK., Cronan, TP. & Kreie J. (2004). *What influences IT ethical behavior intentions-planned behavior, reasoned action, perceived importance, or individual characteristics?* Information & Management 2004;42(1):143-58.

McCormick, M. (2008). *Data theft: a prototypical insider threat*. Insider Attack and Cyber Security 2008;39:53-68.

McCue, A. (2008). *Beware the insider security threat,* CIO Jury, 17/4/08. [Online]
http://www.silicon.com/management/cio-insights/2008/04/17/beware-the-insider-security-threat-39188671/

Moore, A., Cappelli, D., Caron, T., Shaw, E. & Trzeciak, R. (2009). *Insider theft of intellectual property for business advantage: a preliminary model.* International Workshop on Managing Insider Security Threats. West Lafayette, USA: Purdue University.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. (2009).What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems 2009;18(2):126-39.

Ng, B-Y., Kankanhalli, A. & Xu, YC. (2009). *Studying users' computer security behavior: a health belief perspective*. Decision Support Systems 2009;46(4):815-25.

Pahnila, S., Siponen, M. & Mahomood, A. (2007). *Employees' behavior towards IS security policy compliance*. In: Proceedings of the 40th Hawaii International Conference on System Sciences, January 3-6, Los Alamitos, CA; 2007.

Ponemon Institute (2013). *2013 Cost of Data Breach Study* : Global Analysis Benchmark research sponsored by Symantec. [Online]
http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%

205-2.pdf

Post, G. & Kagan, A. (2007). *Evaluating information security tradeoffs: Restricting access can interfere with user tasks*. Computers and Security, vol 26, pg 229–237.

Rantala, R. (2008). *Cybercrime against businesses, 2005*. Technical Report. U.S. Department of Justice. [Online]
http://www.globalinitiative.net/download/cybercrime/north-america/BJS%20-%20Cybercrime%20Against%20Businesses,%202005.pdf

Roman, J. (2014). *Insider Breach Spanned Nearly 7 Years*. [Online]
http://www.databreachtoday.com/insider-breach-spanned-nearly-7-years-a-7267

Sasse, MA., Brostoff, S. & Weirich, D. (2004). *Transforming the weakest link - a human/computer interaction approach to usable and effective security*. BT Technology Journal 2004;19:122-31.

Shabtai, A., Elovici, Y. & Rokach, L. (2012). *A Survey of Data Leakage Detection and Prevention Solutions*. In A Survey of Data Leakage Detection and Prevention Solutions (pp. 5–11).

Son, Y. (2011). *Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies*. Information & Management, 48(7), 296–302.

The State. (2012). *Personal data for 228,000 in SC compromised.*
[Online]
http://www.thestate.com/2012/04/20/2241321_personal-information-of-more-than.html?rh=1

Thomson. (2007). *HMRC data loss leaves 25 million exposed*. ITN News, 22/11/2007

Venkatesh, V., Morris, M., Davis, G. & Davis, F. (2003). *User acceptance of information technology: toward a unified view*. MIS Quarterly 2003;27(3):425-78.

Von Solms, R. & Von Solms, B. (2004). *From policies to culture*. Computers and Security, 23, 275–279

Walker, T. (2008). *Practical management of malicious insider threat - an enterprise CSIRT perspective*. Information Security Technical Report 2008;13(4):225e34.

WFTV (2012). *DCF warns child care workers of possible computer security breach* [Online]
http://www.wftv.com/news/news/local/dcf-warns-child-care-workers-possible-computer-sec/nNPrz/

Chapter IX

9. Appendices

9.1 Abbreviations

PII	Personally Identifiable Information
ISSP	Information Systems Security Policy
IP	Intellectual Property
TPB	Theory of Planned Behavior
DLP	Data Leakage Prevention
HR	Human Resources
PCI	Payment Card Industry
AAA	Authentication Authorization Accounting
DDoS	Distributed Denial of Service
SETA	Security Education Training and Awareness