Internal threat to information security
- countermeasures and human factor within SME

Liene Kreicberga

Luleå University of Technology
Master Thesis, Continuation Courses
Security
Department of Business Administration and Social Sciences
Division of Information Systems Sciences
ABSTRACT

This thesis is based on the viewpoint that no security countermeasure is perfect, each and every one requires some trade-offs to the end user, whether it is limited usability or inconvenience, but as the result of unintelligently implemented security countermeasures errors, carelessness or dissatisfaction among employees may increase internal risk. This thesis is based on theoretical review and one case study.

The research question in this thesis is: How information security countermeasures are perceived by employees and how they change their behavior affecting internal threat level.

To answer that question, this thesis examines various formal, informal and technological countermeasures from the point of end user knowledge and emotional aspects.

The findings of this thesis indicate that formal norms without proper maintenance and awareness do not impact employee behavior, whereas informal norms within an organization have the greatest influence on information security behavior. Technological countermeasures are effective and perceived positively if their necessity is explained as a benefit for end users.

The main conclusion is that the people responsible for information security must identify and assess how end users perceive various information security issues, including the need for and usage of countermeasures, before taking decisions and implementing an information security management system, otherwise information security risks related to internal threat may increase.
# Table of Content

ABBREVIATIONS ................................................................................................................................................. 4

1. INTRODUCTION .................................................................................................................................................. 1
   1.1. BACKGROUND .................................................................................................................................................. 1
   1.2. THE PROBLEM .................................................................................................................................................. 2
       1.2.1. Human factor issues within information security ................................................................. 3
       1.2.2. What is security countermeasure? ........................................................................................... 3
       1.2.3. Why small and medium-sized enterprises? .................................................................... 4
   1.3. RESEARCH OBJECTIVE .............................................................................................................................. 4
   1.4. RESEARCH QUESTION ............................................................................................................................... 5
   1.5. DELIMITATIONS ........................................................................................................................................... 5
   1.6. THESIS CHAPTER STRUCTURE .................................................................................................................. 6

2. THEORY ................................................................................................................................................................. 7
   2.1. INFORMATION SECURITY WITHIN SMALL AND MEDIUM-SIZED ENTERPRISES .................... 7
   2.2. INTERNAL THREAT ........................................................................................................................................ 9
   2.3. END USER SECURITY BEHAVIOR ........................................................................................................... 10
       2.3.1. Knowledge and willingness ........................................................................................................... 11
       2.3.2. Motivation, cause ............................................................................................................................. 13
       2.3.3. How organizations forces employees change their security behavior? ............................ 14
   2.4. SECURITY COUNTERMEASURES AND END USER PERCEPTION ............................................ 14
       2.4.1. Formal policies ................................................................................................................................. 16
       2.4.2. Awareness program, training ....................................................................................................... 17
       2.4.3. Informal norms ................................................................................................................................. 18
       2.4.4. Access control ................................................................................................................................... 19
       2.4.5. Identification and authentication ............................................................................................... 20
       2.4.6. Monitoring, surveillance ............................................................................................................... 22

3. THEORETICAL FRAMEWORK ............................................................................................................................ 24
   3.1. INTERNAL THREAT WITHIN SME .............................................................................................................. 24
   3.2. RELATIONS BETWEEN COUNTERMEASURES AND SECURITY BEHAVIOR ....................... 24
   3.3. INFORMATION SECURITY COUNTERMEASURES .......................................................................... 25
   3.4. HUMAN AFFECT, COGNITION, BEHAVIOR ...................................................................................... 27
   3.5. INFORMATION SECURITY BEHAVIOR IMPACT ON THREAT LEVEL ......................................... 28

4. METHODOLOGY .................................................................................................................................................... 32
   4.1. RESEARCH PURPOSE ................................................................................................................................. 32
   4.2. RESEARCH APPROACH .............................................................................................................................. 32
   4.3. RESEARCH PROCESS .................................................................................................................................. 33
   4.4. DATA GATHERING METHODS ................................................................................................................... 35
   4.5. INTERVIEW GUIDE ...................................................................................................................................... 37
   4.6. DATA ANALYSIS ........................................................................................................................................... 38

5. EMPIRICAL DATA ................................................................................................................................................... 39
   5.1. CASE STUDY ................................................................................................................................................ 39
       5.1.1. Documentation ................................................................................................................................. 39
       5.1.2. Interviews .......................................................................................................................................... 39
       5.1.3. Observations ...................................................................................................................................... 39

6. DATA ANALYSIS ................................................................................................................................................... 40
   6.1. ORGANIZATION .......................................................................................................................................... 40
   6.2. COUNTERMEASURES ................................................................................................................................. 41
       6.2.1. Confidentiality agreement .............................................................................................................. 41
       6.2.2. Information System Security Regulations ................................................................................... 42
       6.2.3. Training, awareness ....................................................................................................................... 44
       6.2.4. Formal process of reward and deterrence ................................................................................... 44
List of Tables
Table 4-1 Qualitative research strategies, adopted from Yin 2003 .................................................32
Table 4-2 Data collection sources, adopted from Yin 2003 ...............................................................36
Table 4-3 Sources of evidences, strengths and weaknesses, adopted from Yin, 2003 ...................36
Table 6-1 Comparison of cognition and affect about countermeasures .............................................59

List of Figures
Figure 2-1 ABC model, adopted from Tipton & Krause 2007 ..........................................................10
Figure 2-2 Factors that influence user security behavior. Adopted from Leach (2003) .............11
Figure 3-1 Relations between threat-countermeasure-human factor-behavior ............................25
Figure 3-2 Theoretical framework. Affect-cognition-behavior ......................................................27
Figure 4-1 Overall process of the research ......................................................................................34
Figure 4-2 Research process for the empirical part ......................................................................35
ABBREVIATIONS

ACL – Access Control List
CERT – Computer Emergency Response Team
CISO – Chief Information Security Officer
CSI – Computer Security Institute
IDS – Intrusion Detection System
IPS – Intrusion Prevention System
IT – Information Technology
IS – Information System
PC – Personal Computer
SIEM – Security Information and Event Management
SIMS – Security Information Management System
SME – Small Medium Enterprises
UPS – Uninterruptible power supply
1. INTRODUCTION

The first chapter of this thesis shortly describes the background of the research topic: what is information security, why it is important, what is internal threat. Then the research problem is shortly described and human factor issues and countermeasures clarified. At the end of this chapter thesis research objectives, question, delimitations and thesis structure are described.

1.1. Background

Information is value, and more and more organizations have realized that information security risks can have a negative influence on business process continuity and public image, relations, can cause financial loss, influence relations with clients and partners and their satisfaction, as well as create the problems with legal authorities in case of non-compliance.

‘Information security is the protection of information and its critical elements’ (Whitman & Mattord, 2008 p.4). Information confidentiality, integrity and availability are the three main characteristics of information security. **Confidentiality** ensures that information is accessed only by those who have privileges. Information **integrity** is the state of being complete and uncorrupted. And **availability** characteristic enables users or other systems to access information (Whitman & Mattord, 2008).

Internal threat has been a hot topic within information security for a few years now. But the statistics about this topic is not particularly pleasant. According to the newest CSI Computer Crime and Security Survey (2009) 51% of respondents believed that they would only incur financial losses in 2008 due to attacks from the outside and not from insider abuse, but an alarming number of 44% have admitted that they have experienced insider abuse 2008, which makes it the second most frequent information security fraud after viruses (CSI, 2009). Also Ernst& Young's latest survey (2009) points out that internal risk is high and even 25 % of respondents have noted an increase in internal attacks and 13% have noted an increase in internally perpetrated fraud.

**Internal threat** is a theoretical possibility that an insider (employee, ex-employee, partner or client) who has or has had an authorized access to the assets of an organization intentionally misuses that access in a way that negatively affects the information security of the organization.

Internal threat is a problem that all organizations are facing, as employee action or ignorance can potentially lead to incidents with severity from a few lost staff hours to negative publicity or financial damage so that the organization may even not survive (Kowalski et al, 2008).

Although some researchers emphasize the idea that internal threat is more pressing than external threat (Leach, 2003), not every organization considers their employees as a serious threat source.

Humans usually are afraid of unknown and do not usually suspect colleagues as potential criminals. So we fear hackers and usually we don't fear those we know well, for example IT support guys, so that can make us react inappropriately when dealing with information security issues (McIlwraith, 2006). But comparing insiders with persons that do not have physical or logical access rights, insiders have more opportunities to easily negatively affect
organization information security (Liu et al, 2009).

On the other hand, if the people responsible are too suspicious and employees are considered as potential criminals, too strict requirements can lead to ignorance, bypassing regulations and dissatisfaction. Security and usability should be balanced, but to find the balance within organization various issues related to threats, risks, countermeasures and humans should be considered. Liu et al (2009) also notice that organizations are struggling with a dilemma of how to protect information that is necessary to share with insiders to perform business processes or support them.

1.2. The problem

To reduce internal threat, the ones responsible for information security usually apply various administrative and technical controls to reduce or mitigate internal threat. But do we understand how threat minimization and mitigation controls are perceived by the employees?

'In trying to implement security policies, practitioners sometimes feel that they are involved in turf wars and personal vendettas rather than rational discourse' (Kabay 2002, p.2).

Some of those responsible for security do consider social psychology in the information security context, but only when information security awareness program is developed and implemented, not during everyday risk management, and security controls are usually selected only based on their cost. However, the attitude of employees to security requirements and controls is affected not only by the security awareness program, but also by several other factors, for example: their own knowledge, the attitude and behavior of other colleagues and management, and also the way information security management system is implemented and maintained.

Information systems security personnel usually have a wide variety of backgrounds, but most of them lack any awareness or training in social or organizational psychology (Kabay, 2002). If the persons responsible for management and security at an organization do not take issues related to employee perception into account, they could under- or overestimate risks, and as the result of inadequate control the impact on employee behavior would even be negative.

Most people have a reasonably positive self-concept; they believe to be competent, moral and smart (Tavris& Aronson, 2007). If organization management and persons responsible for information security tend to make feel people otherwise with their attitude toward employees and implemented countermeasures, employees can negatively impact organization information security. Network traffic monitoring, too restrictive internet access policy or too complex passwords to remember, but writing down is prohibited – these are only a few examples of things that could be unacceptable for employees so that they could try to avoid or bypass them or feel disgruntled. This is one of the key findings of Cappelli et al (2007) - insiders who have intentional intent are usually disgruntled and motivated by revenge.

Internal threat is not only caused by malicious insider who want to stole information for personal gain, various security incidents are caused by employee ignorance, carelessness, or errors. Therefore countermeasure usability, functionality and the way how they are implemented influences internal threat level.

This thesis will research security countermeasures that are used to reduce internal threat and
how employees perceive them and how it changes their security behavior therefore affecting information security within organization.

1.2.1. Human factor issues within information security

Although information security has been considered to be mainly a technical field for many years, lately the importance of how humans affect information security is emphasized and researched.

People are still the weakest security link (Deloitte, 2008). 'We need to remind ourselves again and again that information security is not a technology issue – it’s a people issue' (Colley 2007, p.1). 'Security is both a feeling and a reality' (Schneier 2008, p.1). It is important to recognize that humans have foibles and weaknesses (McIlwraith, 2006). All of previous authors emphasize the importance of human factor within information security.

Within this thesis term 'human factor' is considered as a psychological area that focuses on human mind. According to the Human Institute glossary (2009), 'psychology is the science of human cognition (thoughts, ideas, memory), affect (emotions, feelings), and behavior (actions)'.

Gardner (2008) states that a human is not used to thinking that his feelings are a source of his conscious decisions, but many researches prove that human behavior is affected by cognition and affect. But the human brain is designed with blind spots, not only optical, but also psychological (Tavris& Aronson, 2007). Even those who have knowledge and skills have blind spots and make errors all the time (McIlwraith, 2006).

An employee can contribute with security related actions every day, and his/her view on information security is built on organizational, technological and individual factors (Albrechtsen, 2007). Information security usually has a lot of tradeoffs and mainly it affects functionality – employees have various limitations to perform their duties.

The main problem is that the ones responsible for information security do not take the thoughts, feelings and behavior of employees into account, Kabay (2002) even states that it is common for organization management and people responsible for security not to listen to employees but mainly deal with commanding them. McIlwraith (2006) notices the important characteristics of information security practice within organization – it arouses emotions, sometimes even significant negative emotions.

Unintelligent countermeasures may result in employees behaving in a way that would negatively affect security, because security solutions are developed to attempt to protect information, but the human factor is often left without attention (Thomson et al, 2006).

1.2.2. What is security countermeasure?

To avoid, reduce or mitigate risks related to information security, organizations implement and maintain various mechanisms. Even if those mechanisms are not documented or established by technical means, they exist informally as an internal organization security culture. Controls, safeguards, countermeasures are terms used to describe mechanisms used for information protection (Whitman & Mattord, 2008). Within this thesis, the term countermeasure will be used.

Oxford dictionary (2009) defines countermeasure as 'an action taken to counteract a danger or threat'.

Countermeasures can be categorized in various ways. One way is to categorize them based
on what they do – preventive countermeasure, detective countermeasure or corrective countermeasure. Countermeasures could be categorized also based on their type - administrative, logical and physical.

According to Whitman & Mattord (2008) there are three general categories of countermeasures – policies, programs and technical countermeasures. Policies are setting rules for employee behavior by documentation. Programs are activities that are performed to improve information security – education, trainings and awareness programs. Technical countermeasures are security policies implemented by technical means.

Some of the researchers (Schultz et al, 2001) consider that security countermeasures are only technology and procedures, but others state that informal norms have a serious impact on employee information security behavior and it is possible to manipulate informal norms and thus even reduce internal threat (Frank et al, 1991; Da Veiga & Eloff, 2010).

Da Veiga & Eloff (2010) also show that information security components, information security behavior and information security culture are interrelated. Leach (2003) notices the influence of senior management and colleague behavior on employee security behavior and therefore on internal threat.

Within this thesis not only technological and formal norms, but also informal norms will be considered as countermeasures and end user knowledge and emotional aspects about those countermeasures analyzed to identify security behavior changes.

### 1.2.3. Why small and medium-sized enterprises?

Within this thesis small and medium-sized enterprises (SME) are considered as organizations with less than 500 employees. SME have a few common characteristics related to information security issues and that influences internal threat – small security budgets, responsibility for security being assigned to employees with other duties or only one person is responsible for all information security issues, employees know each other in person, social interactions and strong trust is established among them.

GFI survey (2007) results confirm that 32% of respondents have suffered breach (internal or external) and 42% do not consider their networks to be secure. Internal incident analysis by Kowalski et al(2008) shows that 36% of incidents were reported by SME.

### 1.3. Research objective

As showed by the problem description, information security is not only a technical field and the efficiency of various countermeasures is based on end users who are the main target of these countermeasures and use them every day, so the human factor within information security should certainly be considered during risk management life cycle.

The preliminary literature review revealed that the human factor within information security area is mainly researched from the viewpoint of how humans perceive one specific countermeasure, no matter what organization he/she works for or what information security management system is implemented within that organization. Not many researches have been done in the field of analyzing the information management system of one organization for internal threat minimization and how employees perceive all countermeasures.
The main purpose for this study is to gain knowledge about the human factor within information security area.

The objectives of this research are to identify countermeasures addressing internal threat and analyze end user knowledge and emotional aspects to acquire a deeper understanding on how employees perceive those countermeasures and how employees change their security behavior. The knowledge about employee perception and security behavior changes can help to identify whether there are countermeasures that negatively influence internal threat level.

1.4. Research question

As the result of preliminary literature review to gain the research objectives, the following research question was formed:

**How information security countermeasures are perceived by employees and how they change their behavior affecting internal threat level.**

To reduce the complexity of the research problem and get a better idea of how to approach it, the problem should be divided into smaller units (Leedy & Ormrod, 2005). The problem of this research could be divided into the following sub-problems:

- What are the factors that influence the security behavior of employees?
- How do employees perceive security countermeasures addressing internal threat?

1.5. Delimitations

This thesis has two parts – theoretical and empirical and both parts have delimitations that are described within this section.

The theoretical part contains analysis of various literature sources that describe human behavior and only most well-known security controls that are implemented to reduce internal threat within SME. Based on literature review, theoretical framework is developed to describe most notable relations between countermeasures and end user security behavior.

The empirical part - case study describes the information security management system of a small/medium size organization concerning the internal threat at the moment of data collection. The case study will not be based on analysis of real internal incidents, but on analyzing the threat – a theoretical possibility of an incident. Due to the geographical location, the organization studied in the empirical part will be from Latvia.

This study will be limited only to one organization, its current employees (end users) of the organization, and will not take into account ex-employees, clients, partners or other type of people who could be considered as insiders. Other threats that can negatively affect information security, like hacker attacks, software/hardware errors or failures, forces of nature will not be considered.

Also malicious impact of external persons on employees (social engineering) will not be considered.
1.6. Thesis chapter structure

This research is divided into six chapters and has twelve appendices. Chapter 1 introduces the research problem and describes the research objectives, question and delimitations. Chapter 2 contains a review of various literature sources about countermeasures used to reduce internal threat and how humans perceive those countermeasures. Chapter 3 presents the theoretical framework developed based on the literature review to answer the research questions. Chapter 4 lists the empirical data gathered by documentation analysis, interviews and observations. Chapter 5 contains data analysis for case study based on theoretical framework and empirical data. And finally, Chapter 6 concludes the research by describing the most notable conclusions and provides suggestions for future researches in the area of information security and the human factor within it.
2. THEORY

This chapter contains literature review about information security within SME, internal threat, countermeasures and human perception, behavior. Various research paper reviews and analyses show the importance of internal threat within SME and the relations between countermeasures for internal risk minimization or mitigation and human perception and behavior.

2.1. Information security within small and medium-sized enterprises

Statistics show that major part, even more than 99%, of the economic activity are contributed by SME and internet growth and reliance on information technologies has increased various threats to information security and therefore can negatively affect business (Tawileh et al, 2007; Gupta & Hammond, 2005).

It is important to understand the characteristics of information security within SME to identify threats, assess risks and implement countermeasures. Comparing information security issues within SME and large organizations, there are differences, but it should be noted that there are very few academic researches within area of information security and SME (Gupta & Hammond (2005).

According to Tawileh et al (2007), information security management within SME should be different than within large organizations, and the gap between various sized organizations are direct result of available money, human of technical resources that SME can invest to protect against threats. Gupta & Hammond (2005) consider that comparing with large organizations, major constraints for SME are:

- staff with limited security experience,
- lack of finances to hire external consultants or provide employee training,
- lack of risk understanding,
- inability to focus on security because of need to focus on other business requirements.

Dojkovski et al (2007) focuses on information security culture within SME, and their main findings are: SME has lack of security knowledge and understanding about information security importance within business, minimal reports of security incidents and breaches, lack of IT manager position.

Dojkovski et al (2007) agrees that SME management do not assign necessary time and budget for information security. And Tawileh et al (2007) also notices that SME information security budget usually is usually very tight. But not only information security budget is important difference for SMEs, also lack of awareness about threats and information security issues are common for SMEs (Tawileh et al, 2007).

Dealing within information security issues, SME are mainly reactive not proactive (Dojkovski et al, 2007), there are lack of security strategies. SME also less strictly follow to regulatory requirements (Tawileh et al, 2007) and they have fewer deterrent countermeasures than large organizations (Gupta & Hammond, 2005).
According to Gupta & Hammond (2005) research, majority of SME did not have information security policy in place. This finding also proves other researcher conclusion that SME has limited human resources for security duties and lack of management understanding about information security importance within organization.

Few authors notice the importance of employees and internal threat within SME. Insider access abuse SME consider as the least important among information security threats, although insiders are the most costly and least caught criminals (Gupta & Hammond, 2005). Tawileh et al (2007) state that human factor presence complicates information security issues even more. But Gupta & Hammond (2005) thinks that disgruntled employee could be even the source of attack against information assets, they notices that limited financial resources and expertise within SME can lead to lack of policies and procedures within organization and that can rise the risk of insiders attacks.

Some researchers review efficiency of information security countermeasures within SME, one of the Gupta & Hammond (2005) major findings was that SME quite often chooses to use technologies for security risk minimization that are not very effective for their environment, therefore could cause even more serious risks. This finding also shows the main problem area of this thesis.
2.2. Internal threat

The importance of internal threat is a serious issue that should be addressed with care (Workman et al, 2008). However researchers have different views on what is considered as internal threat and why and how insiders negatively affect information security. Some of them focus on internal threat with malicious intent, for example, Kowalski et al (2008) states that majority (88%) insiders planed their actions. Some even state that major security breaches come from insiders that subvert internal countermeasures (Dhillon, 2001).

According to CERT, internal threat could be categorized (Moore 2008) into three large groups based on motivation:

- theft or modification of information for financial gain,
- theft of information for business advantage,
- IT sabotages.

But Walker (2008) sees also other causes for internal threat – motives as personal gain, revenge, disgruntlement, ideological differences or even accident.

Some researchers (Liu et al, 2009) focus on those insiders who do not have malicious intent, but do not manage information security issues responsibly, but other researchers (Leach, 2003; Dhillon, 2001) describe internal threat as not only internal incident with malicious intent, but any incident that is caused by internal persons, including their errors and omissions. Also Walker (2008) categorizes internal threat into malicious that is intentional and adversarial in nature and non-malicious that is accidental and non-adversarial incidents. Leach (2003) states that poor or unacceptable employee behavior is one of the major causes for security incidents within an organization and not only intentional security attacks, but also user security errors, carelessness and negligence are serious threats to information security. I will agree with this idea because there is no strict border between intentionally performed and unconsciously performed incidents. McIlwraith (2006) also agrees with Freud's idea that even accidents are often the result of our subconscious activity.

So within this thesis any incident caused by internal persons and negatively affecting information security is considered as internal threat.
2.3. End user security behavior

According to Leach (2003), internal threat is mainly the result of poor user security behavior, so to reduce or mitigate internal threat it is important to understand what influences employee behavior. Information security countermeasures that are implemented to reduce and mitigate internal threat can change a person’s attitude and beliefs and therefore his/her security behavior. Schultz et al (2001) also notice the importance of user’s acceptance, willingness and ability to follow the security requirements.

Many researchers agree with the idea that the human mind is composed of rational and emotional components. A few authors state that security behavior depends on a person's attitude and beliefs. Belief is cognitive information without emotional component, but attitude is evaluation or emotional response (Kabay, 2002).

Some other author’s (Tipton & Krause, 2007) propose the ABC model (see Figure 2-1) where employee attitude to information security issues is based on rational component (cognition), emotional component (affect) and behavior:

A – Emotional aspect of attitude, for example, feelings like grief, pain, fear, guilt.

B – Behavior component is derived from fact that our behavior also gives feedback to attitude.

C – Cognitive or thoughtful aspect of attitude.

![Figure 2-1 ABC model, adopted from Tipton & Krause 2007](image)

There are also other ways of categorizing factors that affects security behaviors. A research by Herath& Rao (2009) showed that security behavior can be influenced by intrinsic and extrinsic motivators. Intrinsic motivators comes from "rewards inherent to a task or activity itself" (Wikipedia, 2010), for example, the perceived effectiveness of the security countermeasure. Extrinsic motivators are those that come from outside the person (Wikipedia, 2010), for example social pressure or impact on penalty.

The importance of employee behavior monitoring is emphasized by Kabay (2002), he states that it is necessary to identify to avoid errors of attribution when trying to implement or maintain some security countermeasure. And for avoiding errors of attribution, the first step is to identify why person behaved like that. Kabay (2002) classifies behavior of persons...
according to two independent dimensions – internal/external and stable/unstable. *Internal and stable* behavior is when person usually behave like that. *Internal and unstable* behavior is when person has some extraordinary situation that changed his behavior, but usually he does not behave like that. *External and stable* behavior means that it is other (for example system) behavior that is common and impacted persons behavior. And finally *external and unstable* is behavior that initiated externally, but is not common.

Kabay (2002) state that mostly people behavior is less stable and internal, than stable and external and knowledge about employee behavior category addressing security issues, help to persuade to change their attitude or behavior.

According to Leach (2003) there are two groups of factors that impact employee behaviors – the first group consists of user knowledge about what the organization expects of them, the second group consists of factors that influence employee willingness to constrain themselves to behave appropriately, see Figure 2-2

![Figure 2-2 Factors that influence user security behavior. Adopted from Leach (2003)](image)

**2.3.1. Knowledge and willingness**

Human belief is seriously affected by their knowledge and memory issues. Oxford dictionary (2009) defines knowledge as 'information and skills acquired through experience or education'.

Leach (2003) states that human knowledge (Figure 2-2, upper part) is based on:

- What they are told
- What they see
- Their own decisions
What they are told. This group consists of organization formal statements on information security – policies, procedures, manuals. The effectiveness to impact security behavior lies in body of knowledge accessibility, completeness, clarity of stated values and uniformity.

What they see being practiced by others. Most serious impact on employee behavior is from senior management values and attitudes, consistency between company’s values and other employee behavior, and whether other organization practices reflect to its security values.

Their own decisions that are based on previous experience. It is not possible to describe all possible security decisions within policies and procedures, so every employee time to time is in situation where his own security decision has to be taken, therefore building up his own knowledge base.

Human memory has limited capacity, it decays over time, confuses similar items, has difficulty in recalling non-meaningful items, can not forget on demand (Sasse, n.d.). Memory reliability is a very serious issue that affects our decisions and therefore our behavior, because memory is like an organic process that fades, vanishes or even dramatically transforms, and therefore recent, emotional, vivid or novel events are more likely to be remembered (Gardner, 2008).

Willingness (Leach, 2003) is based on:

- Personal values and standards
- Sense of obligation
- The degree of difficulty

Although people mainly are able to take up and apply the values and rules of an organization, it is possible that there is a conflict between the person's values and standards and values and standards of the organization and then people is tend to follow his values.

Each employee has a so called “psychological contract” with his employer that makes him/her feel a certain pressure to behave according to expectations, especially if the employee is well treated, recognized and rewarded. But if the employee feels untreated by employer, he/she can lose the willingness to act in the interests of the organization or even feel so angry that he/she would wish to punish the organization, therefore the sense of obligation toward the employer influences behavior.

The degree of difficulty they experience in complying with the rules of the organization also influences. If security countermeasures are too difficult to perform or comply, countermeasures seem to be ineffective; even if employees understand that they should follow the requirements, still they have little tolerance to comply.

Other researchers focus on what influences PC security related behavior (Frank et al, 1991). Informal norms – informal and unwritten social norms, especially role clarity and motivation to comply with expectations or demands of organization, affect people security behavior. But if there is a lack of formal or informal norms, users PC skills and experience is the most important factor that positively correlates to security behavior (Frank et al, 1991). One more finding by Frank et al (1991) was that the perceived personal responsibility is important for work results and motivation, but it does not affect security related behavior. The existence of formal policies is expected to contribute to good security behavior by drawing attention and clarifying expectations, but the research by Frank et al (1991) does not prove this positive correlation. Still, formal policies can provide a basis for the development of more effective informal norms.
2.3.2. Motivation, cause

Incident analysis shows that the majority of insiders employed legitimate user commands, but only 23% were employed in technical positions (Yachin, 2006). CERT study (Kowalsky et al., 2008) showed that 90% of insiders were current employees with authorized access at the time of incident. It is notable that almost a half of insiders already showed some inappropriate behavior before the incident, but organization policy violation was not registered (Kowalsky et al., 2008). Cappelli et al. (2009b) also notices that 30% of internal IT sabotages were performed by those who had previous arrest history.

But what were the motives for those insider incidents performed with malicious intent? According to Kowalski et al. (2008), financial gain is the most (54%) important motivator for internal threat. The study also revealed that 24% of internal incidents were performed for revenge and 14% felt specific grievance. Yachin (2006) gives a similar ratio - the motive for most insiders studied were the prospect of financial gain (81%); followed by revenge (23%); dissatisfaction with the management culture or policies of the company, (15%); and desire for respect (15%). The study by Kowalski et al. (2008) also stated factors that affect internal threat and it is noticeable that the majority (56%) of illegal activities were triggered by specific events – termination, transfer or other disciplinary action (40%), personal problem unrelated to the organization (15%), dispute or dissatisfaction with management, organization or its policies (10%).

Although previous authors only review internal incidents with malicious intent, other incidents that are caused by negligence, carelessness are also applicable, so the causes for unintentionally performed incidents should be reviewed. Kraemer & Carayon (2007) consider that the importance of accidental security incident causes is underestimated, because deliberate attacks often are successful only because of internal employee error.

Errors made by humans operating equipment could be categorized into following categories (Anderson, 2008): skill level mistakes that occur when we unintentionally perform a practiced action instead of an intended one, rule level mistakes occur when we follow the wrong rule. And finally, cognitive level mistakes are made when we do not understand the problem.

Some authors (Kraemer & Carayon, 2007) go deeper into cause analysis and extend mistake and error levels into interrelated elements that may create conditions for human error and information security violation: individual elements, task elements, workplace environment elements, technology elements, organizational elements. Although Kraemer & Carayon, (2007) focus on errors and causes identified by network administrators and security specialists, their error model could be adjusted for end user errors and mistakes.

**Individual elements** are those who are specific to the person and include security experience level gained over time, individual assignment of specific tasks within group, individual level of security knowledge based on training, individual assessment of security status, and end user perception.

**Task level elements** consist of job structure, employee job duties and workload.

**Workplace environment** elements include psychical access, noise from other workers and equipment, interruptions by co-workers and equipment disruptions.

**Technology elements** include operating system, inadequate hardware and software, encryption rules, use of diagnostic tools, use of security software and poor human-computer interaction.
Organizational elements include communication, information security culture, policy, implementation, organizational structure, resources, and strategic issues. Kraemer & Carayon (2007) research results showed that organizational elements were the factors that are the most contributive for errors.

2.3.3. How organizations forces employees change their security behavior?

One of the most effective ways to improve information security behavior is an employee awareness and training program. According to Frank et al, (1991) the most important variables that change user behavior and attitude related to information security within the organization are user knowledge and informal norms. Researches show that almost all users agree on the importance of information security and think that training and awareness program is the most important step to improve information security (Albrechtsen & Hovden, 2009).

But there is a gap between employee knowledge and employee behavior (Workman et al, 2008). Sasse (n.d) points out that not only security knowledge, but also motivation, persuasion and social norms have an impact on security behavior. Self-interest and real, believable threats change people's perception and attitude and thus change their security behavior (Sasse, n.d.). Psychologists are of the opinion that reward and punishment are the factors that govern people's actions (Tavris& Aronson, 2007). Literature for educating the ones responsible for information security usually holds the view that employees should be deterred by all three:

- fear of penalty
- probability of being caught
- probability of penalty being applied.

Not only punishments but also rewards are serious motivators for behavior (Kabay, 2002). Also Leach (2003) is of the opinion that rewards for good security behavior is a great way to improve employee behavior. But it is not used very often. By mainly enforcing information protection, organizations focus entirely on punishing those who break the rules (Kabay, 2002).

Instead of focusing on reducing security violations, the emphasis should be on improvements in success (Kabay, 2002). However, some authors do not agree that motivation theory could be useful to reduce employee related security risks because security does not have clear outcomes that could be measured, therefore it is difficult to reward and sanction (Frank et al, 1991).

2.4. Security countermeasures and end user perception

To identify and reduce internal threat, risk management should be performed by a particular person responsible for information security. According to Whitman & Mattord (2008), risk management program has two formal processes - risk identification and assessment and risk control.

As the result of the selected risk control strategies for various insiders caused risks, even if it
is not documented, various countermeasures are chosen and implemented to reduce internal threat.

Cappelli et al (2009b) state that reducing internal threat is possible but it requires complex and layered strategy consisting of policies, procedures, internal culture and technical environment. They propose best practices for organizations to prevent and detect internal threat based on various countermeasures that are provided for end users. Cappelli et al (2009b) state that it is necessary to document and enforce formal policies and controls so that employees receive consistent and clear message about what is prohibited and consequences of violation. Periodic training on policies also should be performed so that employees are aware of security requirements that are stated within documentation. Additionally regular security awareness training for all employees should be performed not only about policies and procedures but also about various information security issues.

Not only preventive, but also detective and reactive countermeasures should be used for threat mitigation. Monitoring as the detective method and mandatory response to suspicious employee behavior as reactive method is necessary (Cappelli et al, 2009b). Monitoring should be performed even before hiring by background checking for all potential employees and during employment personnel should be monitored to identify financial problems or changes in behavior. As employees can intentionally or accidentally disclose confidential information in Internet, also employee online activities require attention, so their activities should be logged, monitored and audited regularly. But it should be mentioned that most of those technologies to control and monitor employees will erode sense of privacy, sense of liberty and responsibility (Frank et al, 1991).

Information security issues should not be viewed separated from overall organization issues, so Cappelli et al (2009b) propose that there is necessary to anticipate and manage issues that can arise during employment, not only related to information security, but all negative workplace issues.

As information should be protected in any form, including, for example, printed or stored in flash memories, and also all technical assets should be physically protected, it is necessary to track and secure physical environment to reduce risk associated with physical access to assets (Cappelli et al, 2009b).

Cappelli et al (2009b) also states that implementing password and account management or other method to enforce separation of duties and least privilege principles are effective ways to technologically limit employee access to information bases on need.

But to minimize the risk of insider threat by leavers, formal procedures should be established for termination procedure and one of the most critical is to deactivate computer access after employee termination (Cappelli et al, 2009b).

Yeh & Chang (2007) have seven categories of countermeasures that are grouped in two groups – IT related countermeasures and non-IT related countermeasures. IT related countermeasures consist of various software, hardware, network and data protection methods, but non-IT related countermeasures – physical facilities and environment, personnel, regulations and risk transference methods. Comparing those countermeasures with Cappelli et al (2009b) proposed, the main difference is additional countermeasure - risk transference.

Some authors contemplate on mechanisms that would ensure that countermeasures for
internal threat reducing and mitigating are effective, because countermeasures can be implemented unintelligently so that employees ignore or try to bypass. There are ways how to improve control acceptance among employees. Joinson & Whitty (2008) thinks that employee input in security rules could increase their acceptance and complying with security requirements. Dhillon (2001) thinks that there are five components for ideal internal threat countermeasure mechanism:

- Control environment
- Risk assessment
- Countermeasure activities
- Information and communication technologies
- Monitoring

Countermeasures or so called control environment consists of actions, policies and procedures and gives the employees a message from the organization management about the importance of information security. Walker (2008) agrees that various organizational and technological countermeasures are necessary to prevent, detect and mitigate internal threat. Dhillon (2001) state that control activities include policies and procedures to ensure that controls are in place. Security policy is among fundamental security countermeasures within regulatory and legality group also in Yeh & Chang (2007) research. Risk assessment is necessary not only to identify and implement countermeasures, but also to identify flaws in internal controls. Information and communication technologies are used to gather transactions and maintain accountability of performed activities (Dhillon, 2001). Yeh & Chang (2007) lists firewalls, ACL, proxies, IDS and antimalware as already outdated technologies and SIEM1, SIMS, Forensic, IPS, gateway protection and content filtering as present technologies for addressing insider threat. If previously Dhillon (2001) proposed mechanisms were mainly for preventing, the last threat control mechanism is only for detecting internal threat - monitoring the quality of controls.

It is very important to choose the most appropriate security countermeasures, because the quality of information security management system and risk perception affects employees' awareness, motivation and behavior (Albrechtsen, 2007).

Frank et al (1991) state there is interaction among user knowledge, formal policies and informal norms. Formal policies and informal norms are most influential when user’s knowledge is low. And knowledge is the most influential, when there are no formal policies and existing norms are weak.

2.4.1. Formal policies
Many security-related tasks could be automated by using technology, but there is employee behavior that can not be addressed by technology and requires security policies (Herath & Rao, 2009). To manage those risks, different security-related documentation is developed, implemented and maintained. Documentation usually defines at least the minimum - security roles, responsibilities, authorized uses of information and systems, prohibited uses, requirements for system management, consequences of violation (Whitman & Mattord, 2008).
Cappelli et al (2009b) say that policies should be clear enough for employees, because internal risk rises if policies and controls are misunderstood, not communicated, or not fully enforced. People need enough time to understand security requirements and integrate them into their everyday behavior (Kabay, 2002).

The main research conclusion by Frank et al (1991) is that formalized policies and procedures for security related issues are unlikely to be effective if not supported by various other actions that increase employees' knowledge and understanding of the necessity of norms.

Effective security policy should be developed based on best practices, distributed by using various methods, read and understood by all employees, agreed and enforced (Whitman & Mattord, 2008). Every policy should be written on a reasonable reading level, wording is important – with minimal technical jargon and management terminology, so that the employee comprehends it (Whitman & Mattord, 2008; Kabay, 2002).

Herath & Rao (2009) state that the objectives of any policy within an organization is to influence the actions of employees, but even if policies are clear and detailed enough, the result is not as expected. This is typical especially regarding security policies, because employees seldom comply with written security norms. Research results by Wiant (2005) show that the presence of information security policy has no impact on the number of incidents or seriousness of incidents.

Security policies and procedures affect not only what employees do, but could initiate emotions like anger about the problems to get their work done. Security policies also conflict with inbuilt social interactions – to help a colleague, ask for advice (Kabay ,2002).

Herath & Rao (2009) within their research on security policy compliance propose incentive mechanisms: penalties, social pressure and perceived effectiveness that his/her security behavior can make a difference in securing information. The analysis of empirical data of research showed the following key findings: the first one is that employees are more likely to follow policies if they perceive their security compliance behavior to have a favorable impact on the organization or benefit the organization. Secondly, social influence is important. If employees see others complying with the security policy, they are willing to comply themselves. And finally, if employees perceive that there is a higher likelihood of getting caught if they violate policies, they are more likely to follow them.

The research by Herath & Rao (2009) showed interesting results regarding penalties for policy violations – the severity of a penalty even has a negative impact on security behavior intentions.

2.4.2. Awareness program, training

The latest survey by Ernst&Young (2009) showed that 74% organizations have a security awareness program, but mainly it covers only security topics in general. Other most popular topics are: review and agreements of compliance with current security policies and standards (61%), direct and frequent updates of threats (44%), updates on new hot topics (42%).

As human judgment is influenced by the manner in which information is presented, Kabay (2002) proposes that employees have a better perception of real life examples and explanations how policies can protect employees against false accusations and the organization from a negative reputation and loss of profit.

Many authors suggest that awareness and training are the most effective ways to reduce
security incidents (Sasse, n.d.). But others do not agree, because researches have shown that users mainly know the requirements and the consequences, but they break some rules to cope with the cognitive and social pressures (Allendoerfer & Pai, 2005). Also a research by Dhamija & Perrig (2001) has showed that the level of security training did not prevent users from choosing trivial passwords and insecure behavior.

The channel used for communication is very important – the most effective medium to get the employees’ attention is face-to-face communication (Kabay, 2002). Employees from a high risk group should receive not only security awareness, but also training. It is also important to explain employers how to identify internal threat source, so experts (Cappelli et al, 2009a) advise that information security training should not concentrate on identification by describing stereotypical characteristics or profiles (for example, gender, age), but rather try to explain how to identify insiders by their behavior.

2.4.3. Informal norms

Every organization has its corporate culture, and it influences employees' security behavior, therefore, information security culture should be integrated into the corporate culture and be a part of employees' daily activities and behavior (Thomson et al, 2006). According Schein (2004, p.17), culture covers all of the given group’s life, but his proposed definition of group culture is ‘a pattern of shared basic assumptions and internal integration, that was worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems’.

A large organizations is more likely to have well specified policies in place (Herath & Rao, 2009), but as this thesis focuses on SME, it is common that parts of documented policies are missing and informal norms have a greater impact on information security. If there are inconsistencies between formal and informal norms, employees are more likely to follow what they see instead of what they are told, so informal norms are more important than formalized (Leach 2003).

Ruighaver et al (2007) consider describing information security culture on the basis of Detert et al (2000) organizational culture framework. Although this framework could not cover all aspects of information security, Ruighaver et al (2007) described following conclusions about each culture dimension out of eight:

- The basis of truth and rationality. Employee and organization belief about security importance and other beliefs about security issues have serious influence on security culture (Ruighaver et al, 2007). That means that if employees see that management and other colleagues do not care about information security, they could also change their attitude.
- Nature of time and time horizon. In organizations with long-term goals and strategic security management, where employees are regularly reminded about their responsibilities, security culture is better and employees' behavior is more secure.
- Motivation. There should be appropriate processes to ensure that employees are motivated to behave securely. Employee motivation could be increased not only by various rewards, but also by social participation in security issues.
- Stability versus change/innovation/personal growth. Employees usually prefer stability over changes, but security usually requires changes, so change management and control should be implemented carefully.
• Orientation to work, task, co-workers. Too much limited access can result in nuisance, so there is a need to find the balance between security and how constrained employees feel. Also it should be noted that if some unsatisfactory behavior is widespread among employees, they usually consider it normal behavior.

• Isolation versus collaboration/cooperation. Quite often security tasks are isolated from day-to-day operations or business processes so the decisions that are made by security management team could be not taken into account.

• Control, coordination and responsibility. Organizations where security goals are not aligned with organization goals, employees are more likely not to support security. Responsibility comes with employee accountability, but it does not mean that delegation of duties will reduce the need of management support and a clear vision.

• Orientation and focus – internal and/or external. If organization focus only on compliance or industry standards or other external requirements, usually employees neglected those requirements rather that if organization is internally focused or focus is balanced.

Ruighaver et al (2007) also notice the importance of top management support. They find that for better employee security behavior management the prioritization of information security should be visibly demonstrated, security issues should be taken into account when planning organizational strategies and support should be provided for an overall security program.

Leach (2003) emphasizes the importance of the attitude of the senior management toward security. Their ignorance and carelessness with information security issues will let employees perceive the security culture within the organization as weak and they will not consider themselves to be duty-bound. Strong leadership creates strong culture and that gives a clear message to all employees about the importance of security (Leach, 2003).

One more issue regarding informal norms within organization is related to human migration and organization employee culture influences. People from various countries can have different cultural backgrounds and can behave differently to proposed security requirements. It is valuable to identify those issues related to cultural background and employee beliefs and attitude before pressing employees to follow (Kabay, 2002).

2.4.4. Access control

Organizations usually face the problem of how to balance between security and usability. Although internal threat incident analysis (Yachin, 2006) shows that 43% of insiders used their own user name and password to carry out the incident, it is important to limit insider’s access to information.

The main problem from the viewpoint of human factor is that access control limitations are against social interaction – we are polite and usually invite even an unknown person to come into the room and try to help. But access control principles prohibit that and require the person responsible for security to be informed (Kabay, 2002).

Separate consideration is required for relations between employee and persons with authority, because the majority of insiders (58%) worked in administrative or support positions and half of them had been assigned supervisory or leadership roles (Kowalsky et al, 2008). One problem with access rights is that it is difficult to assign accurate access right to managers (Post & Kagan, 2006). Very often managers do not even need access rights to IS or server room. If a manager does not have access rights, then employees usually have
serious problems to say “no” when the manager asks for information that he/she is not authorized to access (Kabay, 2002). Allendoerfer & Pai (2005) also notices that employees are more likely to reveal the password to authority just because of not looking too suspicious.

2.4.5. Identification and authentication

Identification and authentication are the fundaments of information security (Schultz et al, 2001), the most used techniques for user access right control and user behavior related password usage area where a lot of research has been carried out. Basically there are three types of authentication systems – something a person knows, for example, password, PIN code, something a person has (key, smart card) and something a person is, for example, its fingerprint, iris pattern (Anderson, 2008).

Knowledge based authentication

Passwords are very often used as an authentication mechanism within SME, but human memory issues and social aspects could make people feel frustrated, annoyed and even disgruntled if a password system requires too much security from users. Keith et al (2007) state that there are three correlated fundaments:

- effectiveness, which refers to password strength from attacks
- usability, which refers to how easy is to remember and enter the password
- satisfaction, which refers to psychological perception that the user has of the effectiveness and usability of password.

Anderson (2008) notices that there are three broad concerns regarding passwords – probability to enter password correctly, whether user remember or write down, and whether user accidentally or intentionally disclose password.

Generally there are two human factor problems within knowledge based authentication from the point of usability. First problem is that password according to its security requirements could be too long or too complex to enter. Second problem – difficulty to remember because of requirements to change too often or too difficult, or there being many systems with different passwords.

Password memorization issues are well researched; for example, Allendoerfer & Pai (2005) address mainly the memorization problem and subdivide it in more detail based on 5 cognitive pressures for user passwords: length, complexity, frequency of change, frequency of use, and number of passwords.

- Length

According to Allendoerfer & Pai (2005) Miller (1956) study showed that human short term memory has a capacity of seven “chunks” plus/minus two. “Chunk” is a meaningful set of information, for example a word. But more than 36% of organizations require passwords to be at least eight characters. If users are allowed to add meaningful data to password, password recall rate significantly increases (Allendoerfer & Pai, 2005).

- Complexity

To reduce brute force attacks, password policy often requires a random password without
words from dictionary, which creates a problem for users to remember them. It elevates
cognitive pressure; especially if users are not aware of various mnemonic techniques for
easier memorizing of passwords (Allendoerfer & Pai, 2005).

According to Allendoerfer & Pai (2005), the main method for remembering random
password is frequent rehearsal or by writing down. Passwords that are written down and
available for colleagues can negatively affect the level of internal threat.

- Frequency of change

Frequently changed passwords are more difficult to crack because of time limitations. Most
often passwords are changed every 30-90 days, but critical applications require passwords to
be changed even more often. But there are give-and-takes – the more frequently passwords
must be changed, the harder they are to remember, because the person is affected by the so
called “proactive interference” – when trying to remember a new password, an older
password is recalled by mistake (Allendoerfer & Pai, 2005).

- Frequency of use

Usually there are passwords that we need to enter many times every day, but also there are
passwords that we need to enter once in a month or even more rarely. Those passwords that
are used everyday are easier to remember than those used rarely (Allendoerfer & Pai, 2005).
Sasse (n.d.) even proposes that different authentication mechanisms could be considered for
frequently and infrequently used passwords.

- Number of passwords

Surveys have shown that employees usually need to get authenticated in many systems, but
one of the cognitive pressures is that the more passwords a person needs to remember, the
more difficult it is to remember any specific password and there are more chances of
interference among similar passwords, (Allendoerfer & Pai, 2005).

Using fewer passwords could reduce unacceptable cognitive pressures for users without
serious password security reduction, so management should allow using the same password
for different systems (Allendoerfer & Pai, 2005).

Allendoerfer & Pai (2005) notice that not only the cognitive pressure impacts employees,
but also the social aspects and user attitude affects the behavior related to passwords. Some
of these aspects are: identity, trust, informal work procedures. The research emphasizes that
humans are social by nature, so they tend to be viewed positively by themselves or
colleagues and do not want to be labeled as “nerds” because of not sharing passwords or
revealing information to a colleague if they are asked for it. Also employees often perceive
password sharing as a sign of trust between colleagues, but trust is important for teamwork
(Allendoerfer & Pai, 2005) and usually organizations try to establish trust within necessary
groups. As a result, if an employee is asked for his/her password, he/she would feel a social
pressure to reveal it.
Password management system requires changing a password when it is lost or an account is blocked. Even if the password reset process is easy, the employee will experience some frustration and will lose his productivity in case the password is forgotten or the user account blocked due to entering a wrong password too many times (Allendoerfer & Pai, 2005).

**Token based authentication**

Token based authentication is used not only for user authentication within IS, but also for physical access control. Tokens usually have some kind of a password to authenticate the user, usually a PIN code, and it creates the same problem as with passwords, the only difference being that a PIN code is shorter and usually does not require to be changed so often. Authentication tokens have human factor weaknesses similar to password systems, because users may forget, misplace or damage their tokens and the result will be almost the same (Allendoerfer & Pai, 2005). But Schultz (2007) states that a token based system has a few more factors that affect user behavior, because it requires additional steps to authenticate and therefore authentication time increases and more errors could be generated.

**Biometrical authentication**

Biometrical authentication systems are more expensive and therefore not so often used within the SME sector.

From the usability perspective biometrical authentication is less extensive than token based system, but more extensive than passwords in the terms of steps required for authentication (Schultz 2005). The less steps, the less pressure for users. Authentication based on biometrical parameters has one advantage over other authentication systems, because users are not required to remember password or keep track of a token (Allendoerfer & Pai, 2005). Also Sasse (n.d.) notices that biometric solution could reduce the mental workload, but still there could be specific problems with usability, for example – which finger do I need to put in the fingerprint reader, where to look in the iris recognition system? Some technological problems, especially false rejection of authorized users and delays could increase workload and cause frustration for users. Privacy issues are important, so the idea that the employer is collecting and storing sensitive information about employees could make feel them uncomfortable. But it seems that biometrical systems are becoming more and more acceptable among users (Allendoerfer & Pai, 2005). Systems usability is affected by various permanent or temporary user physical changes, which also affects system crossover error rate.

2.4.6. **Monitoring, surveillance**

Employee monitoring is often implemented by technological means, as network traffic monitoring or video surveillance, because new technologies and cheap data storage has shifted from only suspected person surveillance to mass surveillance (Joinson & Whitty, 2008). Although monitoring from the point of managers and information security personnel is mainly considered as a very effective detective countermeasure against internal threat, it could deter users from malicious behavior, but monitoring also can have some harmful effects (Joinson & Whitty, 2008).

It is not practical to look at what everyone is doing; instead specific patterns of behavior should be monitored (Cappelli et al, 2009a). According to Wakefield (2004), surveys have shown that 82% of companies use some type of electronic monitoring; most popular are
Internet connection monitoring (63%), e-mail (47%), computer files (36%) and video recording job performance (15%). But other survey results, for example, E-crime survey (n.d., 2007) show that surveillance is considered as one of the least effective controls. It should be noted, that although monitoring is becoming more popular, some behavior can not be monitored, like writing down passwords or sharing them (Herath & Rao, 2009).

Internet usage and email monitoring is often used to monitor and control the waste of productivity (Whitty, 2004), but actually it can lead to poorer task performance (Joinson & Whitty, 2008). The same situation could be within internal threat – if too much monitoring and video surveillance is used, employees could feel distrusted and disgruntled. According to Whitty (2004), Irving et al (1986) found that employees who are monitored have greater stress, decreased satisfaction and quality of relationships compared with non-monitored employees. Survey (Whitty, 2004) results showed that 19% are opposed to any kind of Internet filtering in the workplace.

Computers are the property of the organization, and organization holds the responsibility for their usage, but some employees perceive computers and internet usage as more traditional modes of communication, like telephone conversations, and think that Internet usage should be acceptable for private purposes (Whitty, 2004).

Privacy is a very complex issue; a considerable amount of researches has been conducted in the field of surveillance and user perception, mainly from the viewpoint of employee privacy. For example, people perceive Internet and e-mail communications as a more private channel than face to face or telephone conversations (Witty, 2004). Although some papers consider monitoring as a totally necessary means to fulfill compliance requirements, and legal experts even advise that a working place should have no privacy at all and no one should be trusted (Wakefield, 2004), the legal issues of privacy in working places differ in every country. Privacy International (n.d., 2007) state that some countries have even directly or indirectly prohibited or restricted monitoring. The idea that the employer has no rights to monitor everything could significantly reduce employee satisfaction and rise disgruntle. Network traffic and video monitoring are countermeasures so invasive on privacy that they are not accepted by everyone, so these should be addressed very carefully. One of the discoveries is that people with greater perception of vulnerability to security threats and perception of organization procedural justice have a more positive attitude toward monitoring (Workman, 2009). Transparency of personal information protection measures and how monitoring is performed improves employee attitude (Workman, 2009).

Another issue that should be mentioned is trust. Trust as a psychological contract is very important within organizations, but monitoring could create a feeling that everyone is a potential criminal. The level of trust is important; if employees trust those who collect, process and store their data, the issues of privacy are less pressing (Joinson & Whitty, 2008). But generally, surveillance reduces the trust in a workplace (Joinson & Whitty, 2008).
3. THEORETICAL FRAMEWORK

This chapter contains the description of the theoretical framework used in this study. The theoretical framework for this study was derived from the literature review above. The literature review helped to understand the problem and guided to data gathering and analysis. The theoretical framework describes two variables and how they are related and how they impact human behavior: (1) information security countermeasures within an organization to minimize or mitigate internal threat and (2) end user perception of those countermeasures. The relations between both of these variables will be used to answer the research question.

So this research was carried out in two phases: in the first phase information countermeasures were identified and analyzed. In the second phase the human perception of those countermeasures was analyzed. The theoretical framework shows that there are various countermeasures that influence user information security behavior and further empirical study should be performed to prove the negative/positive influence.

3.1. Internal threat within SME

After literature reviewing, the thesis problem area and following characteristics were identified within SME information security:

- lack of understanding about insider threat and risks
- limited human resources for security management
- lack of understanding about the importance of human factor
- other priorities over information security

3.2. Relations between countermeasures and security behavior

As the result of literature review to answer research question, the following relationships are detected between internal threat, countermeasure, human factor and security behavior (Figure 3-1).

To reduce internal threat, various security countermeasures are implemented and maintained, but the way employees' understanding of these countermeasures influences their behavior are not always clear. So within this thesis perception of information security countermeasures by end users is researched.
3.3. Information security countermeasures

In order to examine the research question, various researches were reviewed within the theoretical part with the aim to identify and describe information security countermeasures that are used to reduce and mitigate internal threat. Based on the literature review, all information security countermeasures could be derived from the following groups:

- Formal countermeasures
- Informal countermeasures
- Technological countermeasures

Documentation and established formal processes that regulate employee behavior related to information security issues are called formal norms or formal countermeasures. At least minimal documentation or statements signed by employee within his/her job contract, job contract appendix or information security policy is necessary to enforce employee security responsibilities and regulate employee behavior. The way documentation is implemented and maintained also is important, because training and awareness program impacts user knowledge and therefore behavior. Various formal processes of reward and deterrence for good or bad security behavior change employee attitude toward information security issues.

Informal countermeasures are non-written rules, beliefs, attitudes that exist in an organization as internal culture and have a significant influence on employee behavior. The most serious influence is from what people see (Leach, 2003), so end users change their security behavior also based on other co-workers and management security behavior.

Technological countermeasures are various physical and logical solutions to identify, limit and monitor non-acceptable end user behavior. As was identified within the theoretical part, the main groups of countermeasures are: access control (physical, logical) for limiting access on need to know basis and implement the principle of separation of duties, authentication (password based, token based, biometrical) for identification and establishing access rights, and monitoring (physical, logical) for detecting internal threat.
To answer the research question of how employees perceive countermeasures, the following basic countermeasures will be analyzed within this thesis:

- **Documentation related to information security.** Every organization has some kind of internal documentation whose main objective is to influence behavior (Herath & Rao, 2009). Most often basic security requirements are set in the job contract and security policy procedures. Documented norms must describe employee responsibilities, authorized uses of information and systems, what behavior is prohibited and consequences of violation (Whitman & Mattord 2008).

- **Training and awareness.** Training and awareness provided for employees raises knowledge about security issues and also influences the emotional aspect of how information security is perceived by employees.

- **Every organization has some kind of reward and deterrence process to prevent employees from unacceptable behavior, like being late or not fulfilling duties.** So if information security incidents and reaction to these incidents is integrated into the overall reward and deterrence process, besides, this process is effective, employees will improve their security behavior.

- **Internal security culture.** Ruighaver et al (2007) conclusions about eight culture dimensions will be used as a framework to identify and assess internal culture. The management and co-worker belief about importance of information security, the goals and strategy set for information security, the motivation for good security behavior, stability and changes within organization, focus on team work and social interaction, security issue isolation, responsibility and control over employees, and finally, internal or external focus. All previously listed factors have a significant influence on end user security behavior.

- **Access limitations.** A very effective way to reduce internal threat is to implement access rights based on “need to know” or “least privilege” principle within internal IS. Also Internet limitations are used to reduce the possibility of information leakage. Physical access limitations can help to secure information in paper form and IT assets from physical threat – stealing, damaging.

- **Identification and authentication.** User names, passwords, smart cards are technological countermeasures that are most often used within SME to identify end users and authenticate them to enforce access limitations and provide accountability.

- **Monitoring.** As not all risks caused by employees can be prevented, monitoring should be implemented to identify unacceptable employee behavior for later reaction. Monitoring can be implemented by various ways – IS usage monitoring, Internet access monitoring, physical employee behavior monitoring.

The theoretical framework shows that there are various formal, informal and technological countermeasures for preventing and mitigating internal threat that require analysis of user perception and security behavior to ensure that internal threat level is not raised because of
unintelligently implemented or maintained countermeasures.

3.4. Human affect, cognition, behavior

The literature review showed that the majority of authors consider the human factor to be based on two aspects. To answer the research question, the cognitive (knowledge, awareness) and affect (emotions) aspects will be considered within this thesis as those that change human behavior (Figure 3-2). Both aspects will not be separated; they will be seen as a one inseparable entity instead and the term “perceive” will be used within this thesis for that entity.

![Figure 3-2 Theoretical framework. Affect-cognition-behavior](image)

Both aspects are interrelated and based on personal experience, knowledge and memory issues, management and co-workers attitude, willingness to comply personal values and standards, sense of obligation, difficulty to comply with requirements, motivation and various emotions (anger, guilt, fear, and grief).

Within this thesis internal threat is considered as theoretical possibility of any incident caused by internal persons that negatively affects information confidentiality, integrity or availability, including intentionally performed attacks, unintentional errors, carelessness and negligence (Leach, 2003).

Within this framework, human errors classification is based on skill-rule-knowledge model by Rassmusen (Anderson, 2008; Kraemer & Carayon, 2007), where errors are categorized based on an individual’s level of performance - skill level, rule level or cognitive level. Skill level mistakes appear when an end user becomes inattentive during the performance of routine tasks and does not notice that there are changes that require attention and different action. If the employee must make a decision and as a result he chooses the wrong rule, then a rule level mistake can occur. Cognitive level mistakes occur because of end users' insufficient knowledge about the necessary security behavior.

It is important to follow security requirements and everyone should concern and take care of security issues. Negligence and carelessness include lack of common sense, forgetting or knowingly ignoring security requirements, taking inappropriate risks (Leach, 2003).
Attacks performed by internal end users can be based on various motivations - personal gain, revenge, grievance, disgruntlement, desire for respect, ideological differences, business advantage, dissatisfaction with management, culture or policies (Walker, 2008; Moore, 2008; Kowalski et al, 2008; Yachin, 2006).

As a result of literature review, the following factors are considered as causes for internal threat level raise that could be influenced by end user behavior: skill level error, rule level error, cognitive level error, negligence and carelessness, motives for personal gain, revenge, grievance, disgruntlement, desire for respect, business advantage, dissatisfaction with management, culture or policies.

3.5. Information security behavior impact on threat level

As was mentioned within the theoretical part, poor security countermeasures can create cause or motivation for security attacks, errors, negligence or carelessness and thus raise internal threat level.

Based on the literature review, the following countermeasure initiated behavior changes related to this theoretical framework can be identified: documentation, training and awareness process, process of reward and deterrence, internal security culture, access control, authentication, and monitoring.

3.5.1. Documentation

The way how documentation regarding information security is developed and implemented impacts user knowledge and affect and therefore security behavior. There is a certain minimum that should be defined to enforce security requirements (Whitman & Mattord, 2008), but there is no defined maximum of requirements that an employee can perceive and follow.

But it should be noted that documentation can have a negative impact on information security behavior. Formal documents that regulate behavior can increase dissatisfaction with management and policies.

The content of these documents is important - if there are too many requirements, written in difficult language with specific terms, without simple definitions, the employee may misunderstand, may not understand at all, may not remember or enforce them in everyday life. Too strict or too many requirements for employee security behavior can lead to problems with performing job duties, can make them feel untrustworthy, annoying and unsatisfied. A human is a social being, so overly strict requirements can conflict with other managerial processes that are implemented to improve efficiency within an organization, like team building and social interactions with co-workers.

The process of implementing and maintaining documentation is very important. It is difficult for a human to change his/her usual behavior, so implementing documentation in a hurry can lead to various errors and dissatisfaction. If management or the responsible persons do not give a clear message about the importance of following those norms during implementation and maintenance process, the employee may not see the benefit to follow.

Regular reminders help to move good security behavior knowledge into skill mode or unconscious mode, otherwise if requirements are not regularly reminded, a human is tended
3.5.2. Training, awareness process

As mentioned previously, good security knowledge requires regular reminding; training and awareness programs are an effective way of improving security knowledge. Nevertheless, also negative training and awareness program influences on end user knowledge and feelings and therefore on security behavior are possible.

The content of the training and awareness programs is essential. Security issues, if addressed in an overly complicated way, may lead employees to misunderstanding and disturb their judgment. Influence on intimidation can help to deliver message about security risks, but also can make employees feel stressed and afraid of taking decisions.

The way training and awareness process is organized and presented is important, so special attention should be paid to the fact that training and awareness does not disturb somebody from duties and the process is enjoyable, not boring.

3.5.3. Process of reward and deterrence

Deterrence process is an effective way to persuade employees to follow security requirements and behave securely. Fear of being caught and penalty applied can be a serious motivation change and can also reduce errors, carelessness and negligence. But there is also the other side of deterrence process – too much focus on intimidation may decrease trust and respect level, increase dissatisfaction about the management and its policies.

A reward procedure can change employees' attitude to behave more securely, if it is clear and reasoned, otherwise it may increase grievance or other negative emotions about oneself being underestimated but a co-worker – overestimated.

3.5.4. Internal security culture

Within this research the Ruighaver et al (2007) model will be adopted as a framework for internal culture dimensions.

Management attitude toward end users and information security issues has a serious impact on the overall satisfaction of employees and therefore on good behavior. Other colleague and managements ignorance and carelessness against information security issues influences each end users behavior negatively. Some unacceptable behavior, for example, password sharing or ignorance to follow security requirements could be copied from co-workers.

The way information security changes are implemented has an impact on end users – notable changes implemented in a hurry would not be accepted by end users. People need time to understand the need for changes, accept them and establish them as everyday behavior.

Responsibilities and duties within information security management system need to be reminded often, otherwise knowledge-based errors, negligence or carelessness will increase.

Another serious issue is trust and cooperation among co-workers. If trust among employees is very strong, then internal access control limitations could fail, because everyone will share the data with co-workers.
3.5.5. Access control

Access control systems allow implementing separation of duties, the least privilege principle, limit and control employee performed activities within public networks and limit physical access to critical information and technical assets. Too restrictive access control may make an employee feel encumbered, untrustworthy or try to bypass them, thus endangering information security even more. The inbuilt need for social interactions with co-workers (Kabay, 2002) can conflict with strict access limitations and lead to violated access right.

Internet access limitations can prove to be good in guaranteeing that employees are not spending their time browsing the web and reducing the possibility to download prohibited information or send confidential data, but Internet limitations will also influence employee satisfaction.

Physical access limitations that require regular inconvenience can be bypassed by, for example, putting something in doors, asking a colleague for token, thus increasing negligence and carelessness.

Employee knowledge and any system usability issues can seriously influence various employee errors within a system that affect threat level.

3.5.6. Identification and authentication

End user identification and authentication is necessary to implement access control and provide later accountability of employee actions. If authentication requirements (the number of passwords, password complexity, changing frequency) are too difficult for employees to remember or enter, then passwords will be written down and even kept in a visible place, it could raise the risk that colleagues may use others' passwords for unacceptable activities. IS session will not be cancelled or operating system will not log-off when leaving working place, if passwords are too difficult.

If token based authentication requires a kind of password or PIN code to authenticate user to smartcard, then all previously described password problems apply. Additionally, physical factors, for example, too difficult procedure for authentication (close proximity reader not adjusted for human height), lost or forgotten card at home, easily breakable cards can make feel dissatisfied and employees could start to look for ways to bypass.

If password entering and remembering is difficult, as a result user account may be blocked and require to be reset and smartcard require to be reissued. Too bureaucratic password reset or token reissue procedures may disrupt work duties, make employees annoyed and dissatisfied.

Biometrical authentication additionally has various usability and privacy related issues; user acceptance of, for example, iris, retina or fingerprint scanner, is different and should be considered before implementing, otherwise, dissatisfaction will increase. Additionally, crossover error rate should be analyzed to guarantee that authentication is free of false rejection issues.

Skill level mistakes are seriously influenced by authentication systems that are developed or implemented unintelligently, because authentication system usability influences human errors.
3.5.7. Monitoring

As not all internal risks can be entirely avoided, mitigating strategies usually are implemented. Monitoring employee behavior by various means is an effective way to identify unacceptable security behavior, but too much control and monitoring may step over employees' sense of privacy and lead to stress and dissatisfaction about work conditions, which in its turn may negatively impact employee motivation, willingness to comply to requirements and overall security behavior.

Monitoring also raises the feeling of distrust, but trust between employer and employee is an important factor for good behavior. Monitoring can also raise fear from accidentally unacceptable behavior; it can reduce social interactions and trust among co-workers.

It is almost impossible to separate all working hours from private life, so employees could feel that internet and email could be used for personal interest, therefore network traffic monitoring may result in employees disgruntlement or they could use some external anonymous proxy server to encrypt data flow, which it raises the risk of various other attacks and malicious software.
4. METHODOLOGY

The purpose of this chapter is to describe the research methodology used in this thesis. The first two sections describe the purpose of the research and the approach. At the end of this chapter thesis research data gathering and analyzing methods are described.

4.1. Research purpose

The purpose of this thesis is to identify the information security countermeasures that SME use to minimize or mitigate internal threat, and the way employees perceive and understand information security issues and countermeasures. Knowledge about internal threat and how security countermeasures are affected by the human factor could help to lately choose the most appropriate control mechanisms and therefore reduce the risk level or mitigate the impact.

According to Yin (2003) determining the research questions is the most important part and requires specific preparation, for example, like reviewing the existing literature. As a result of preliminary literature review, the main question of the research was determined to be:

How information security countermeasures are perceived by employees and how they change their behavior affecting internal threat level?

4.2. Research approach

Research methodologies can be categorized into quantitative and qualitative research methodologies. Quantitative research methodology is used within researches that either identify the characteristics of phenomenon or explore the possible correlations among phenomena (Leedy & Ormrod, 2005). But all qualitative researches have two things in common – they focus on “real world” phenomena and they are used to research that phenomenon in all its complexity (Leedy & Ormrod, 2005). Table 4-1 shows the how various qualitative research strategies differ and how to choose the most appropriate method based on the form of the research question, control possibilities over events and the time of event occurring.

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Form of research question</th>
<th>Requires control of behavioral events?</th>
<th>Focuses on contemporary events?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case study</td>
<td>How, why?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Survey</td>
<td>Who what, where, how many, how much?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Experiment</td>
<td>How, why?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Archival analysis</td>
<td>Who what, where, how many, how much?</td>
<td>No</td>
<td>Yes/No</td>
</tr>
<tr>
<td>History</td>
<td>How, why?</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Case study research methodology is used to study a particular individual, or a program, or event in-depth studies; it is especially suitable for learning about poorly understood situations (Leedy & Ormrod, 2005). Comparing case study methodology with other quantitative methodologies, like, experiments, surveys, histories and analysis of archival information, the case study is the preferred method when “how” and “why” questions are being posed, when there is little control over events, and focus is on contemporary event within real life context (Yin, 2003).

This research problem could be studied using either qualitative or quantitative methodology, but I think that the most appropriate is to research the phenomenon security countermeasures against internal threat and employees in depth by using case study research methodology. According to Yin (2003), case studies are used to contribute or knowledge of individual, group, organizational, social and related phenomenon.

This thesis will have two parts – theoretical and empirical. The theoretical part will focus on internal threat analysis from the viewpoint of the available controls to reduce or mitigate internal threat and how employees perceive security issues and controls. The empirical part will consist of one case study in which an existing information security management system will be described and data from employees will be gathered and analyzed about how they perceive it and how it affects security threat level.

According to Flyvbjerg (2006) case studies could be used to generate hypothesis and to test hypothesis. As this research is limited to only one case study, it will not test, but rather build up problematization.

### 4.3. Research process

The overall process of the research, consisting of sequenced steps as shown in Error! Reference source not found.
Within the preparation step, preliminary analysis of various literature sources was performed to identify the possible problem areas.

The next step was to define the research problem, objectives, questions and delimitations. As the result in the first chapter of this thesis the research problem, objectives, questions and delimitations are described.

The third step was to review literature to identify and describe possible countermeasures and human perception and aspects of behavior. As the result Chapter 2 of this thesis was developed that outlines literature review and Chapter 3 for theoretical framework.

The fourth step was to define the methodology to be used for research. After analyzing various methodologies, case study research strategy was choose.

The fifth step is empirical settings and data. A more detailed process of the empirical part is outlined in Figure 4-2. It was possible because the literature review provided valuable knowledge necessary for the empirical part of this research.

The sixth step was analysis of data and comparing to the theoretical part for finding patterns.

And finally, the last step was to develop conclusions and describe future research possibilities within sixth chapter.

Figure 4-1 Overall process of the research
4.4. Data gathering methods

One of strengths of the case studies is that they involve a full variety of evidence – documents, artifacts, interviews, observations (Yin, 2003). For this research, qualitative data will be gathered and analyzed as extensive data is necessary for case study research (Leedy & Ormrod, 2005). To minimize criticism over case study methodology, it is necessary to design good case studies, collect, present and analyze data fairly (Yin, 2003).

The major tasks in collecting data are (Yin, 2003):

1. to gain access to an organization and/or interviewees
2. to have the necessary resources to perform the case study
3. to develop the procedure of calling for assistance and guidance
4. to make a schedule for data gathering
5. to provide for unanticipated events

So to obtain the empirical basis, data will be gathered from organization in the form of documentation analysis, interviews and observations.

Data collection sources can be individuals and organizations, and if the case study is an individual, then conclusions can not be based entirely on interviews, data from the organization also should be used. The same applies to a reverse situation – if the case study is an organization, then data from individuals is necessary (Yin, 2003).
Table 4-2 Data collection sources, adopted from Yin 2003

<table>
<thead>
<tr>
<th>Study conclusions</th>
<th>From an individual</th>
<th>From an organization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>About an individual</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Individual behavior</td>
<td>Archival records</td>
</tr>
<tr>
<td></td>
<td>Individual attitudes</td>
<td>Other reported</td>
</tr>
<tr>
<td></td>
<td>Individual perceptions</td>
<td>behavior, attitudes and perceptions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>About an organization</td>
<td>Personnel policies</td>
</tr>
<tr>
<td></td>
<td>How organization works</td>
<td>Organization outcomes</td>
</tr>
<tr>
<td></td>
<td>Why organization works</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

According to Yin (2003) there are six sources of evidence – documentation, archival records, interviews, direct observation, participant observations and physical artifacts. If data is collected properly, it is likely that there will be a large amount of documentary evidence that is an important part of the case study (Yin, 2003), so data will be added as appendices for this research.

Table 4-3 Sources of evidences, strengths and weaknesses, adopted from Yin, 2003

<table>
<thead>
<tr>
<th>Source of evidence</th>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>Stable, unobtrusive, exact, broad coverage</td>
<td>Low retrievability, biased selectivity, reported biases, deliberately blocked access may occur</td>
</tr>
<tr>
<td>Archival records</td>
<td>Stable, unobtrusive, exact, broad coverage, precise and quantitative</td>
<td>Low retrievability, biased selectivity, reported biases, deliberately blocked access may occur, privacy issues</td>
</tr>
<tr>
<td>Interviews</td>
<td>Targeted, insightful</td>
<td>Bias due to poorly constructed questions, response bias, inaccuracies due to poor recall, reflexivity</td>
</tr>
<tr>
<td>Direct observation</td>
<td>Reality, contextual</td>
<td>Time consuming, selectivity, reflexivity, cost</td>
</tr>
<tr>
<td>Participant observations</td>
<td>Reality, contextual, insightful into interpersonal behavior and motives</td>
<td>Time consuming, selectivity, reflexivity, cost, bias due investigator manipulation</td>
</tr>
<tr>
<td>Physical artifacts</td>
<td>Insightful into cultural features and technical operations</td>
<td>Selectivity, availability</td>
</tr>
</tbody>
</table>
As a result of the research methodology and data gathering method analysis, chosen the following methods will be used within this research:

- **Documentation review**
  Each organization has documentation that describes its information security management system (for example, policy, procedures, guidelines, awareness program) that should be reviewed to identify the controls that are related to internal threat. To describe Case, data within official Organization web site is used.

- **Interviews**
  It should be noted that the nature of interview is much more open-ended, because interviewers do not always cooperate and answers to all questions (Yin, 2003). Personal interviews will be performed with responsible persons and end users. Interviews with persons responsible for specific tasks of the organization are necessary to identify non documented countermeasures. Interviews will provide ample information about the existing information security management system, the controls used, possible incidents, consequences, employee attitude, etc. Interviews will be performed also with employees and will help to understand their knowledge of information security and the way they understand and perceive implemented security countermeasures implemented.

- **Observations** will help to gather additional data about employee attitude toward information security and behavior. Although case studies need not always include direct, detailed observations as the source of evidence (Yin, 2003), observations will be gathered during interviews as additional data for empirical studies. Observation notes are written within Interview transcripts.

4.5. **Interview guide**

According Leedy & Ormrod (2005), case study requires extensive data on which investigation is focused. Interviews are essential source of data within case study methodology especially if humans are investigated (Yin, 2003).

Data gathering in case study methodology should have formal plan, but during data collection specific information could be relevant that could not be predictable before and therefore require additional data (Yin, 2003). Within this case study major data were gathered by interviews, therefore the questions and interview procedure are important to provide qualitative data for later analysis.

Interview taping provides more accurate rendition of interview, but recording devices should not be used if interviewee refuses or appears to be uncomfortable (Yin, 2003). As during interview arrangement some persons expressed negative attitude against interview taping and were willing to be as anonymous as possible, to ensure better response and more open answers from persons, interviews were not taped, but written as the notes. To provide anonymity for interviewees, they are not identified in thesis but to differentiate them interview notes contain only labels A-H.

Totally eight individual interviews from 27 January 2010 to 27 April were performed to gather necessary data for this thesis about current countermeasures and employee perceptions.
Firstly, three semi-structured, open-ended interviews were performed with persons responsible for information security, information technologies and human resources. Some questions were identified in advance, but some during the interview as Yin (2003) propose for case study interviews. Within interview there were questions about security countermeasures under their responsibility. After interview, notes were written and send to interviewee for verifying and his corrections lately reconsidered.

Secondly, structured interviews with five end users were performed; there were 40 questions, the research objectives were used as the guide for questions. Interview questions are outlined in APPENDIX A. Questions could be grouped into following groups: about working experience within Organization, about information security knowledge, about existing formal norms, about internal security culture and how they perceive technological countermeasures. According Yin (2003), although within case study most commonly interviews are open-ended by nature, still more structured interviews could be used.

4.6. Data analysis

Data analysis consists of examining, categorizing, tabulating, testing and otherwise recombinating evidences to address the research problem (Yin, 2003).

Leedy & Ormrod (2005) proposes data analysis based on Creswell (1998) spiral that describe how to treat raw data to get the result – final report. The first step is to organize the collected data by filling, computerizing and braking into smaller units. Second step is to peruse all the data to get an overall sense of data. Thirdly general categories should be identified and data must be classified. And finally, data should be integrated and summarized to be understood by readers.

Within this research will be used general analytic strategy and pattern matching technique that is recommended by Yin (2003) as most desirable technique that compare the empirically based pattern with predicted one.

According to Leedy & Ormrod (2005) data could be organized into tables, figures and other ways of presentation to exhibit information in compact way. Data analysis chapter of this thesis contain detailed description of countermeasures and human perception, additionally for easier comprehension and pattern identifying there is two dimensional table (Table 6-1) inserted with coded and grouped information. For instance, some countermeasures (access control, smart cards, monitoring) contain only ‘positive’, ‘negative’, ‘neutral’ or ‘no opinion’ data codes. Other countermeasures have more descriptive codes that show the each respondent’s general opinion about countermeasure.
5. EMPIRICAL DATA

This chapter contains case study empirical data that were gathered and are used for analysis.

5.1. Case study

5.1.1. Documentation

Following documentation that is directly related to theoretical framework and could be classified as primary data was gathered in electronic form (see Appendices B-D):

- Document template “Employee Contract Confidentiality Agreement”.
- Document “Information Systems Security Regulations”.
- Document “Organization Employee Satisfaction Survey results analysis”.
- Data from Organization web page.

5.1.2. Interviews

To identify and describe countermeasures for internal threat reducing and mitigation, there were performed three interviews. To identify end user knowledge and feelings about various countermeasures, there were performed five interviews.

- Responsible for information security (Interview transcripts see Appendices E).
  Person responsible for information security explained various issues about information security management system and all security countermeasures.
- Human resources manager (Interview transcript see Appendices G).
  Human resources manager explained the process of employee hiring/firing process, employee deterrence and reward process, employee internal culture and overall satisfaction about working condition.
- Deputy Director of IT department (Interview transcripts see Appendices F).
  Deputy Director of IT department explained various issues about information systems, their usage and some technological countermeasures that are used for end user controlling and monitoring.
- Five employees that could be considered as end users (Interview transcripts see Appendices H, I, J, K, L).

Interviews were performed individually in separate room and lasted ~35-45 min. Employees were asked about their information security knowledge, and how they perceive various formal, informal and technological countermeasures.

5.1.3. Observations

Observations were performed during interviews with end users about employee knowledge and attitude toward various issues discussed. Observation notes are written within interview transcripts (see Appendices H, I, J, K, L).
6. DATA ANALYSIS

In this chapter empirical data is analyzed and compared with the theoretical part. The first part of the chapter shortly describes the organization profile and analyzes its countermeasures that were identified during documentation analysis and interviews with personnel responsible for them. Then follows the analysis of how each of the five end-users perceives the previously identified countermeasures. And finally the results are compared and analyzed.

6.1. Organization

The Organization is a state stock company whose objectives are to maintain and develop legal and high quality services and systems for vehicle tracking and control, driver qualifications in areas under national and public interests of the airline industry. It deals with the registration of vehicles, examination of drivers, driver’s licenses issuing and revoking, periodic vehicle technical inspection, and supervision of roads. Financial review of year 2007 showed turnover about 28.8 million EUR, profit almost 1.8 million EUR.

The Organization has one central office, the residence of the main administration, and 26 regional offices, almost 500 employees in total. An important focus of the organization is to improve client service, so it regularly implements new services for clients and tries to improve the existing ones. Another factor that urges changing things is regular legislation changes.

Organization is responsible for two state information systems that have about 100,000 external users – other governmental institution employees, employees from various businesses, and inhabitants of the country. IS has many external interfaces with other governmental institution IS. Additionally few internal information systems (e-mail, internal web, accounting, etc) are maintained to support organization duties.

Within IT department there are 15 employees; one of them has been assigned the responsibility for information security. Personnel and quality department has 5 employees who are occupied with employee management and service quality.

There has been no malicious information security incident performed by insider officially registered within the organization. However, the interviewees said that they remember a few incidents caused by employees, in some cases their employment was even terminated after that. The person responsible for information security is of the opinion that employees can negatively affect internal information security intentionally or unintentionally. During empirical data gathering there was a serious information security incident within another governmental institution and some negative publicity about a potential security breach within the organization that affected the emotions and knowledge of the employees and therefore the empirical data.
6.2. Countermeasures

Although the organization was founded almost 20 years ago, information security issues have only been considered in the past few years, when a person responsible for information security issues was delegated. Information security manager is a delegated role for a person from IT department whose main duty is database management and he can spend about 20% of his time on information security management issues.

Safety, financial loss, inability to deliver business processes and negative publicity are the main reasons to provide information security within the organization, so information security risk management should be applied to all business and support processes, as well as countermeasures for risk reduction, mitigation or transference should be chosen.

After the interviews with the people responsible for information security, human resources and Information Technologies, the following countermeasure groups were identified within the organization:

- **Formal norms**

To be compliant and to minimize information security related risks a set of internal documents has been developed and delivered to end-users and formal processes have been established. The organization has very few documented policies and procedures related to information security, the employees mainly act according to their own knowledge about information security. Every employee must sign a Confidentiality agreement and follow Information Systems Security Regulations. Although Information System Security Policy has been developed, it has not been approved and delivered to end users, so it is not counted as countermeasure yet.

- **Informal norms**

According to the interviews (Appendices A-C), employee turnover is very low (only ~5% per year) and there are very strong informal norms established among them. Many business processes require team work; these people have been working together for many years and trust each other. The person responsible for information security thinks that employee attitudes are different – some are loyal and very careful, but others are careless and inconsiderate in working with information or technical assets.

- **Technological countermeasures.**

Various physical and logical countermeasures were identified – identification/authentication systems based on user name/password, physical access limitations based or smart cards, access right limitations to organization information systems and Internet, network traffic monitoring, video surveillance.

For a more detailed analysis the following countermeasures directly related to theoretical framework could be identified:

6.2.1. **Confidentiality agreement**

The document “Confidentiality agreement” is an appendix to the employment contract and is signed by the employee during the employment procedure. The Confidentiality agreement describes what type of information is considered to be confidential, what would be the result...
of violating the agreement and the employee signature approves that he/she will observe and comply with all rules within the Organization.

The document consists of one page, it is clear and most important parts are pointed out. The Confidentiality agreement is considered to be a base document for enforcing other documented norms within the organization.

6.2.2. Information System Security Regulations

The document “Information System Security Regulation” was developed according to the local legislation requirements for State information systems 5 years ago. The document is enforced, as employees must sign that they have read it, understood it and will comply with it.

This document was developed before Security Policy, so now it should be reviewed to eliminate duplications and contradictions. As the document name states, its content concerns only information within IS, not information in any form.

Although the document is not very detailed, its more than 30 pages cover almost all information system security issues that are necessary to know for each employee within the organization regardless of his/her duties and responsibilities, so some chapters are not for end users but for IT support or management.

The document contains the following chapters that concern end user behavior that could be related to internal threat minimization and mitigation:

- Terms and acronyms used within the document.

Different terms are explained for user comprehension – what is IS, e-mail, firewall, user, commercial notification, user ID, password, audit trail, physical security, information assets, IS threat, IS security, logical security, and technical assets at the organization.

The description of the term “IS threat” is based on the notion that it is not only deliberate but also accidental action that may change, damage or destroy information or technical resources, or unauthorized disclosure. Although not very clearly explained, still this term includes internal threat.

- The scope of this document.

This chapter has a high level description of document scope and a statement that all employees must follow this document.

- Information classification

This chapter is not related to end user responsibilities or behavior.

- Responsibility categories within the organization.

The role of IS user and requirements are described: what he/she must know and understand (documents, requirements, contact persons, conditions of use), how he/she can use the assets, what activities can he/she carry out, the necessity to report possible incidents, the need to attend training.

Various information security roles (owner, custodian and user) and responsibilities according to roles are described. That may help to implement the “separation of duties” principle and reduce internal threat level as well as help end users to understand how
should they behave, based on their role.

- IS asset creation, adding, changing, processing, transmission, storage, recovery and disposal procedures;

The only requirement that concerns the end user within this chapter is that he/she must be compliant to manufacturer’s requirements, restrictions on copying, intellectual property law and all internal documents.

- IS asset restoration procedure;

Users must immediately notify the responsible persons in the case of a problem.

- The arrangement of system information and technical resources usage and control;

The requirements within this chapter are related to internal threat minimization. Copyright and license requirements are explained once more for users, prohibited activities are described in detail, including the use of inappropriate or illegal information or information materials, unauthorized applications and software, inefficient use of resources, unauthorized use of hardware, equipment and materials, prohibition of distributing classified information and security parameters, prohibition of copying and transferring information assets.

- The procedures for providing access to system information and technical resources.

The authorization process is described and what user are allowed/prohibited to do with theirs credentials and access rights, requirements for user ID and password. It is also stated that users are not allowed to use technical assets for private interests.

- Procedures for using and storing information or data necessary to access system information and technical resources;

This chapter contains a description of how users must not store or reveal their passwords. But there are no recommendations how they can create, remember, store their passwords. Every password must consist of at least 8 characters, it should be changed every 90 days, and it is not allowed to be disclosed. A password should not be a known word from a dictionary or related to personal life. All requirements are based on well known practices to minimize and mitigate information security threats.

- The procedure for using and storing information and data necessary to access system.

The requirements for password and user ID are explained once more, but there are inconsistencies with the previous chapter – for example, here the password change time is less than 60 days.

- The procedure for monitoring system security threat emerging signs.

Within this chapter users are prohibited to endanger IS security, perform password guessing, disclose any information about systems.

- The procedure for detecting and managing system security incidents.

Virus infection is the only incident type that is considered within this chapter, and it does not require user involvement.

- The training and knowledge testing of the employees in the field of system security.

Every employee's duty is to inform someone responsible if he/she notices IS security threat, inconsistencies within documentation or conditions that encumber working within
the organization.

The document is developed according to the local legislation requirements and ISO17799:2005 standard; its chapters are named and organized based on external requirements, not for its readers. It is notable that the document requires review and correction, because there are inconsistencies, duplications and incorrectly chosen chapters. The original document contains 32 pages, half of them contain various rules and requirements that the end user must know and follow. Those requirements are distributed all over the document, it is not clearly stated which rules apply to all users and which ones to privileged users with different security responsibilities (IT support, management). The document is written in complex language, not all terms are described clearly.

It should be noted that the document describes security requirements for the information system, not information in any form, so some areas could need additional regulations.

Observations showed that although within interviews end users did not show knowledge about source of security requirements (documentation) and very detailed knowledge about what is allowed and what is prohibited, overall impression was that they have integrated the most critical security requirements in their every day’s behavior while performing their duties, so that information is not disclosed outside the Organization.

6.2.3. Training, awareness

Training and awareness process is necessary to keep users informed and remind the most important requirements. According to the Information security manager, he has performed an information security training two years ago, but not for all employees, mainly the middle management.

Every employee receives an instruction about job duties during employment process and every year there are seminars to refresh knowledge and gain new information about changes. End users have good PC skills, they accept new system changes quickly and do not need training. There is a well-established process of changing management and making employees aware of job duties or changes in IS usage, but information security awareness and training is not provided regularly.

6.2.4. Formal process of reward and deterrence

The Organization has implemented various monitoring methods for detecting unacceptable behavior and has a well-established process of investigation and punishment. There is a separate anti-corruption department that manages the process.

As the result of an investigation, the employee in question is officially reprimanded or even a firing procedure may be initiated. The process and the result of unacceptable behavior are visible for other employees so it also has a preventive effect.

There is formal annual reward process that evaluates employees. Reward process does not evaluate information security behavior, but only overall employee work performance and client references. As the Organization has had limited finances for the last few years, the award is not money but a diploma in which the management expresses gratitude for good work within the Organization.
6.2.5. Internal security culture

The employee turnover rate within the organization is very small and a strong internal organizational culture has been established and affects information security behavior. The organization is distributed; its main central office with administration and top management is in a different location than end users.

- Employee beliefs about the importance of information security.

Information security has not been a hot topic within the organization. As the organization administrative personnel are physically separated from other employees, end users do not see top management behavior or attitude on an ongoing basis. The importance of information security is not expressed so end users do not receive a clear message what is significant and how everyone should behave. Mainly their behavior is affected by closest co-workers and is based on personal experience, ethics, and sense of responsibility.

- Nature of time

There are no set long time goals for information security, all activities for information security are chaotic and based on the responsible person's workload and some external triggers. Employees are not regularly reminded about their responsibilities and security requirements.

- Motivation

There is a process for annual employee rewarding, but it does not review information security behavior, end users are motivated for being good employees – knowledgeable about most important legislations and rules, able to use systems without errors, delivering a good client service. Although this annual evaluation partly also covers security issues (for example, knowledge of Personal data protection law), still there is no emphasis on information security behavior.

The human resources manager and the person responsible for information security are of the opinion that a major motivation for good behavior could be the fear of loosing the job. As the organization is a state stock company it offers stable work places with a guaranteed salary, and all that against the background of a severe economical crisis and a high unemployment rate in the country. Organization has an Anticorruption department that serves as deterrent object, because it carries out formal procedures and applies sanctions to those who violate the rules.

- Stability versus changes

The organization is improving all the time, but the changes are mainly related to its client services and information system functionality. Information security requirements, policies, procedures, technological countermeasures have not changed for a few years.

- Orientation to work, task, co-workers

Employees require a lot of teamwork to fulfill their duties; they also need to ask each other for help because of limited access rights. Therefore a strong trust is established among co-workers and some prohibited behavior, for example, sharing a computer with access credentials, is widespread among employees. The person responsible for information security even indicated that within some departments co-workers share all computers without operating system passwords and also revealed that he thinks password sharing to be common.
• Isolations
Information security formal norms (policies and procedures) are isolated from other processes, but technological countermeasures are not separated from other business processes.

• Control/responsibility
The organization has tight control over what employees are doing, but not specifically from the point of information security. Responsibilities are clearly stated within documentation, but not implemented in the internal culture of the organization.

• Internal/external focus
Organization information security has an external focus – information security countermeasures are implemented to fulfill legislation requirements. Internal risk identification and assessment had not been the source of security requirements.

6.2.6. Passwords
According to the person responsible for information security, the majority of end users have at least 6 passwords – PC boot password, Windows password and various internal and external IS passwords – some of them used every day, some very rarely. But employees can change some local password requirements so that there is no need for entering them.

Password policy is not very strictly implemented for assets of the organization – it only requires 6 characters, IS does not verify passwords against complexity requirements and does not automatically remind that password should be changed.

Many end users have to use not only internal organization systems, but also many external IS that provide access for data, and those systems are owned by other organizations and have other security requirements. So as a result employees may even have 8 passwords that are necessary for providing their duties. On the contrary to the local password policy, external password requirements are very strict and they are implemented by technological means, so end users at the organization must comply with them.

If some internal password is forgotten, the employee has to call the IT support to reset it and get new one, but employees rarely forgot their passwords.

6.2.7. Smart cards
The organization has implemented a smart card system to limit physical access for employees and separate internal usage areas from client service areas. Smart cards do not require entering a PIN, they only require being put near the reader. There are no spare cards available officially, for example, at administrative personnel or security guards, so in case an employee forgets his/her card, he/she needs to ask for a co-workers smart card.

6.2.8. Access right limitations
Physical access right limitations are implemented by using a smart card system, some rooms are accessible for certain department employees, and other rooms are available for all employees. The archive where all sensitive information in paper form is stored is accessible only to a few employees. The IT center is accessible only to IT support personnel.
IS access right limitations are effective way to limit employee access to only that information that is necessary to perform job duties, so within the organization all users have access rights based on need, with the “least privilege” principle implemented. There is a well-established authorization process – if an employee needs to change access rights, his/her direct manager initiates a request for that.

There are limitations for accessing Internet resources by using proxy server black lists, some very popular social sites are denied, and limitations are regularly reviewed and new ones are added, for example, external proxies that employees use to access restricted sites. But these limitations are implemented mainly for reducing nonproductive work, not with the idea that it would reduce the possibility to send out information.

6.2.9. Monitoring

If previous countermeasures were mainly for preventing internal threat, then monitoring is considered necessary to identify employees that behave inappropriately. Within the organization the following monitoring countermeasures are implemented:

- Video surveillance
  The organization uses video surveillance system at client service points, main office and other more critical areas. The system was implemented to protect assets, reduce corruption and solve various conflict situations with clients. The system records video and sound in very good quality, it is possible to identify person and what is said. Recordings are visible for security guards, managers and the Anticorruption department personnel. Although the primary reason for recording is to identify and later prove that an employee has violated some internal rules and to solve conflicts with clients, it may be used for monitoring unacceptable information security behavior.

- Main business information system monitoring
  As there are too many users and too few support personnel, so it is not possible to perform continuous close to real time DB, application or data flow monitoring, so the organization mainly focuses on logfile back-up analysis when suspicious behavior is identified. As third parties often ask for some suspicious behavior analysis from logfile, IT personnel analyses logfiles and sometimes finds also other unacceptable behavior.

- Internet access monitoring
  Although employee activities are logged within proxy server logfiles and logfiles are backed up, but as IT support personnel are under a great workload, the activities are not regularly reviewed, but only in cases of possible incidents.
6.3. How users perceive countermeasures

In the interviews five end users described their how they perceive various countermeasures that are used for reducing and mitigating internal threat at the organization. The names of end users and other demographic information are not provided within research as anonymity must be provided. Only the length of time of working within the organization was asked, because it reveals when the employment procedure were accomplished, all security related documentation explained and how often training or awareness program activities have been performed. The impact of internal culture on a newly-hired employee is different that those who have been working at the Organization for a long time.

6.3.1. End user A

End user A works for Organization 3.5 years, he feels stable within organization as an employee and is quite satisfied with overall working conditions, colleagues and management attitude within branch office. His knowledge about information security is related to personal data protection, he knows what personal data is and that should not be given to third parties, but sharing among colleagues are common, because strong trust among colleagues are established so that he helps if colleague asks for that. And he does not consider that colleagues could harm system intentionally or unintentionally.

End user A does not know who is responsible for information security within organization and all security requirements for his behavior.

Countermeasure perception analysis

- Confidentiality agreement

As it is signed during employment process, end user A has signed confidentiality agreement 3.5 years ago, but he does not remember the fact of signing, such a document at all and what was within it.

- Information System Security Regulations

End user A remembered that there are some security related regulations, and he know how to find, but he thinks that know only approximately what was in it.

When Information System Security Regulations were presented during interview and asked opinion about understanding, remembering and feelings when reading, end user A thinks that document is too difficult to understand because of terms and language and feels that there are too many norms to follow.

- Training and awareness

And user A had not attend training related to information security, but remembered the instruction after employment procedure. He thinks that trainings are not the most effective way, but once a year could be valuable, especially if important subject is give in interesting way.

He regularly receives emails about changes in system or legislation, but about security issues very rarely, so his behavior is mainly based on what others do.

- Formal process of reward and deterrence

End user A is afraid of being caught and that formal process within Anticorruption department is initiated. It motivates for better behavior.
He thinks that existing reward procedure does not concern employees within his department, but only those who’s work result could be evaluated; therefore this process does not affect his behavior.

- **Internal security culture**
  End user A understands the importance of information security and he thinks that his colleagues also understand, but he is not sure whether management also cares about that, because have not heard a clear message from management about responsibilities, requirements. The only thing that is reminded regularly is password change. End user A considers that his motivation to behave securely is not based on documented norms, but on personal sense of responsibility and fear from penalty.

Employee thinks that existing changes within Organization are acceptable, because they are small. Maybe changes are too often, but still do not create a problem. Processes within Organization are organized so that lot cooperation with colleagues is necessary, but as relations with colleagues are very good, it is does not cumbersome to help a colleague or ask some help from them.

- **Access limitation**
  According end user A, his access rights are customized according job duties, but still sometimes need additional rights, so he asks colleague to help. Internet limitations does not bother, because no time for internet browsing. There are few rooms where he can not access, but sometimes need to go, so there is need to ask the help for colleagues again. But everyone is used to that.

- **Passwords**
  End user A requires two passwords for fulfilling job duties and he does not have problem remembering or entering. He knows that passwords should be changed regularly, but systems do not automatically require to change, so it is left to users sense of responsibility and his manager that sometimes reminds. But otherwise he would prefer to have automatically reminders.

Password complexity does not make problems because he has not experienced that system rejected potential password because of noncompliance.

End user A indicated problem with log-off system. He understands that should do that when leaving working place, but sometimes he forgets that, but system does not logoff automatically. But his opinion is that in case of system misuse, video surveillance will show which colleague has come to computer and used system.

- **Smart cards**
  End user A has not problems smart card system, it works well and even if card is forgotten home, colleagues will help and let in.

- **Monitoring**
  Video surveillance is considered as 50:50 positive: negative. Although he already used to video surveillance and feel it invisible, still it affects behavior, for example does allow talking with colleagues freely when no clients. But still end user A consider that everyone has rights of privacy in working places, because it is not possible to remove personal life issues from working hours. But IS and network monitoring does not bother End user A, because he does not act inappropriately.
Conclusion about end user A cognition, affect and behavior

Cognition
End user A understands information security as protecting organization-owned personal data from outsiders. He does not know who is responsible for information security or all security requirements. He thinks that everything prohibited are not available, therefore everything available is allowed.

Affect
Overall satisfied, during the interview did not report serious issues that could be motives for intentional attack.

Behavior:
Although End user's A behavior is not perfectly secure as he does not log off, shares data and accesses it with colleagues, does not choose a secure password nor change it as necessary, he did not have enough motives for intentional attack.

The possibility of skill level errors is minimized, but cognitive based errors are higher, because of lack of security knowledge.

As End user A did not know security requirements and reported some unacceptable behavior, negligence and carelessness can impact internal threat level.

6.3.2. End user B

End user B works within branch office for about 7 years and now feels stable as an Organization employee, only salary is not sufficient, but still he consider that top management, branch office management and direct management cares about employees, but other employees within central office does not understand branch office employee problems and therefore their attitude is not so good. He emphasizes that co-workers within Organization are the best he ever has, he trusts colleagues and do not consider that they could be a threat to organization information.

Countermeasure perception analysis
  • Confidentiality agreement
End user B works within Organization for 7 years, and he does not remember such a document at all.

  • Information System Security Regulations
End user B said that they have so many documents, that he only can recall only a little bit what was in this document, but he knows were to find it.
End user B after viewing Information System Security Regulations thought that it is not readable for ordinary employee, because it seems to be for different level. He considers that this document is developed only to be used in conflict situations, not in every day.
This document does not conform to real life, and if management will try to implement, it would be very difficult, because employees will not change their behavior just because of this norms. And if too many limitations will be, people will start to find how bypass them or feel very unsatisfied.
• Training, awareness
End user B thinks that trainings are valuable way for gaining knowledge, and the most reasonable seem to have training once a year. He has not received information security training, but he remembered online instructions that are available, but those instructions are too long and difficult to understand.
He noticed that within Organization there are email system used for delivery news to employees and he reminds some email about security issues about ½-1 year ago. Email system helps to gain knowledge, also colleagues help with advice, and some knowledge are got by personal experience, so End user B does not consider security knowledge as missing problem within Organization.

• Formal process of reward and deterrence
End user B thinks that he is not afraid of being caught after unacceptable behavior, because he does nothing prohibited.
He has received reward as a good Organization employee, and thinks that it gave good feelings and motivation to improve even more.

• Internal security culture
End user B does not have opinion about management’s attitude to information security issues, because management has not talked about that, but he considers that security issues are not separated from other business processes. End user B thinks that his co-workers are not a threat to information security, because of limited duties and therefore access rights and because of control over employees. His main motivation for acceptable behavior is situation within country (huge unemployment rate), he performs his job without violence of rules, and therefore he is not afraid of being caught in unacceptable situation. He has experienced Organization reward procedure, felt positively about reward, but still he considers it is too bureaucratic process.
The changes within organization are slow and do not problematic for him, cooperation with colleagues is necessary to perform the duties.

• Access limitation
His access rights are limited, so sometimes need to ask manager for help, but it is not annoying. Other colleagues do not bother him for IS access, because he has minimal access rights.
End user B does not think that Internet limitations are reasonable, because employees try to find other ways to bypass restrictions and therefore other threats will be introduced from non trusted external proxy usage.
There are few rooms that are not available, but he does not need to get there.

• Passwords
End user B has to use 2 passwords within systems, and it does not make problems for him, direct manager often remind to change password. But he thinks that system should automatically ask for changing.
Password reset in case of forgotten requires only one call and is very easy and fast procedure.

• Smart cards
End user B considers smart card access system as a good way to protect employee
belongings, because job duties require being out of office quite often. And in case of forgotten card, colleagues always help.

- Monitoring
End user B thinks that monitoring even can have advantage, for example when there is conflict situation with client. Then recording could be watched to prove that that was not employees fault or guilt. End user B thinks that employee has rights on privacy, but Organization restrooms are without surveillance, so employee can go here for personal conversations. IS and Internet monitoring does not bother him, because he thinks that does not do something prohibited or important.

**Conclusion about end user B cognition, affect and behavior**

**Cognition**
End user B knows who is responsible for information security, but does not know all security requirements.

**Affect**
End user B feels good within the organization; he did not report negative emotional factors caused by countermeasure that could drive to unacceptable behavior.

**Behavior**
There is a small possibility that End user B may perform an intentional attack motivated by some internal countermeasure. The possibility of skill level errors is minimized, but cognitive errors are applicable because of missed knowledge.
End user B can be negligent and careless as he does not know what good security behavior is and is mainly influenced by co-workers.

### 6.3.3. End user C
End user C works for Organization 6 years and his feelings are more positive than negative related to being employee of Organization. He thinks that management within his branch office tries to improve overall working conditions, but main management that resides in different part of city does not care about them. There are collegial relations among co-workers, because of video surveillance system, so they communicate only about work issues and do not feel free.

**Countermeasure perception analysis**

- Confidentiality agreement
End user C does not remember that he signed confidentiality agreement and what was within this document.

- Information System Security Regulations
End user C did not remember Information System Security Regulations, because he thinks that there is so much documentation to read and sign, that it is impossible to recall every one. But he knows were to find all necessary documentation in case of needed.
End user C after viewing Information System Security Regulations thought that those they
are difficult to understand and are threatening. He is sure that these requirements are not followed now because all processes are organized totally different, but if organization will try to enforce those norms, he would feel like criminal.

- Training, awareness
End user C has not attended Information security training, but he remind that some seminar encompass personal data protection issues. He got his knowledge about news in Organization from emails that are almost every second day, but he could not remember some security awareness email. So knowledge about what is allowed to do and what no he got from colleagues, manager and also personal experience helps. End user C thinks that training could be valuable way of gaining knowledge and he proposes one training day per year as the best solution.

- Formal process of reward and deterrence
End user C is afraid of being caught so it improves his motivation for good security behavior. He knows that some employees have been fired because of unacceptable activities. End user C does not have opinion about reward process efficiency; he thinks that deterrence is more effective from preventing incidents.

- Internal security culture
End user C does not think that management cares about information security, his opinion that it is just an employee initiative. He is quite sure that employees will not harm systems, because of various control mechanism, therefore employees are not the most important threat, but third parties who has access to systems, but out of Organization control. He thinks that his main motivation for good behavior is ethics and understanding how job should be done. There were fired some persons for unacceptable behavior, so fear of loosing job is also a good motivation.

End user C thinks that changes within organization is small, but requires rapid accepting from end users, and sometimes it is cumbersome to change the habits so fast. He notices also the problem of change management within Organization, is that those who prepare changes do not take into account end users.

- Access limitation
End user C thinks that his access rights are not sufficient, and his colleagues very often disturb with help request. End user C needs Internet access for job duties, so he would like to access all websites without limitation. He indicated that colleagues are trying to bypass this countermeasure by using external proxies. Physical access limitations are not troublesome, because with smart card End user C can access all necessary rooms.

- Passwords
End user C has 6 passwords to use, and main trouble is to create them, because of various complexity requirements for external IS. Organization IS does not have complexity requirements, and password reset procedure for internal systems are easy, but for external systems annoying and takes a lot of time.

- Smart cards
End user C likes smart card system; he thinks that it is maintained for employee protection, but also for some kind of employee control. In case of forgotten card he can use colleague help.

- Monitoring
End user C thinks that video surveillance is mainly protecting employees from conflict situations with clients. He does not bother that his IS usage and Internet traffic are monitored, because he does not do secret operations.

Conclusion about end user C cognition, affect and behavior

Cognition
End user C has some knowledge about information security. He knows who is responsible and that there are a few requirements for information security, but his knowledge covers only a part of what is necessary.

Affect
End user C reported that he feels more positive than negative; some signs of dissatisfaction based on countermeasures were identified. He is unsatisfied and annoyed mainly by disturbance from colleagues to help with accessing IS and password management.

Behavior
Although End user C is partly unsatisfied with some of the countermeasures and therefore could be motivated for intentional attack, the fear of losing the job is a good deterrent factor.

Skill level errors are minimized, but rule-based and cognitive errors could be a threat because of the lack of knowledge of end user C. Negligence and carelessness also is important as he is not aware of what is expected.

6.3.4. End user D
End user D works within Organization for 10 years and feels that Organization as state stock company offer stability and almost guaranteed job. He has never seen top management from central office within his branch office and he thinks that they are too segregated. But local, branch office management understands employees and their attitude are great. Relations among closer co-worker are very good, especially because after last year lay off, where all newer employees were fired, everyone knows everyone for long time and teamwork is pleasant.

Countermeasure perception analysis
- Confidentiality agreement
End user D remembers the fact of signing during employment procedure, but could not recall what was in this document.

- Information System Security Regulations
End user D said that he remembers Information System Security Regulations and think that know stated norms within document. After viewing Information System Security Regulations, he thinks that the language is too
difficult to understand, but such a document should be understood rather than remembered. He also stated that these norms are not followed and even now, just after reading, he could not take seriously these norms, because those who wrote (central office) themselves do not follow this document. As an example he noticed that password length requirement is not followed by IT personnel who assign 5 character passwords, instead of 8.

- **Training, awareness**
  End user D has not attend training about information security, but only seminars about job duties, his knowledge are gained by asking colleagues and from e-mails. End user D likes the process of awareness by email, because he considers it the best way if employees can read email any time. He does not think that there is need for training about information security issues at all, because everyone knows already everything.

- **Formal process of reward and deterrence**
  End user D is not afraid of being caught because he thinks that he performs only those actions that are necessary to fulfill job duties. He thinks that reward process is not necessary, because all employees are used to work with sensitive data and their security behavior is good.

- **Internal security culture**
  End user D think that Organization management cares about information security issues, and employees will not negatively affect information security. He emphasizes the trust among employees and that no one is suspicious about colleagues. Motivation for following internal requirements is driven by existing situation - stable job, good colleagues. End user D is no afraid of being caught, because he is sure that does not do anything without acceptable reason. He does not think that rewarding procedure could improve information security. He thinks that the way how changes are implemented within Organization is difficult for end users, because information about changes are received at the last moment and only most serious changes is known before, from rumors.

- **Access limitations**
  End user D is satisfied with authorization process, he changed position shortly and all access rights were updated according need. Colleagues ask for help, but very rare. End user D hold a view that there should not be Internet limitations, because employees are busy and job duties does not allow to useless spend a time in Internet. There are few rooms not accessible with End users D smart card, but it is very occasional, so colleagues help.

- **Passwords**
  End user D has to use 4 passwords, and he is used to write down passwords, otherwise remembering all of them are too difficult. The only requirement for password is frequency of changes, but as it is left on employee sense of responsibility, many do not change regularly passwords, or sometimes just forget to change. But in case of password reset, the procedure is easy and does not bother.

- **Smart cards**
  End user D perceives smart card system as for protecting employees and their belongings. It
is usable and convenient, but in case of forgotten card, colleagues will help.

- Monitoring
End user D feels terrible about existing situation with video surveillance. Although this system was implemented with a clear message from management that it is only for employee protection from conflict situations with clients, right now they act totally different. They threaten employees that will analyze every word and make a clip for presenting mistakes. And client speech sometimes even not hear-able, so no way to resolve conflict situations. This continuous monitoring is very unpleasant.
End user D thinks that employees has rights of privacy, but surveillance and other forms of control, like Internet monitoring does not let feel good at organization.

Conclusion about end user D cognition, affect and behavior

**Cognition**
End user D is not aware of a responsible person and a majority of security requirements, but he thinks that his knowledge about information security is sufficient. Some of the security requirements he considers to be unimportant and ignores.

**Affect**
End user D feels very unsatisfied about monitoring within the organization, is of the opinion that video surveillance is not only disruptive on privacy but even humiliating. He also has problems with authentication and remembering passwords.

**Behavior**
Some unacceptable security behavior was identified - password writing, sharing access rights. As end user D has very negative emotions about video surveillance system, his dissatisfaction increases and therefore internal threat by intentional attack is increased.
Skill level errors are not serious threat, but cognitive errors, negligence and carelessness are serious as knowledge is not appropriate and internal culture has strong influence on behavior.

6.3.5. **End user E**
End user E works for Organization 6 years, he feels good as employee and although has no relations with management, think that they has good attitude toward employees. He considers that they have good team within department, although everyone is human that could feel bad some day.

**Countermeasure perception analysis**
- Confidentiality agreement
End user E could recall the fact of signing, but not what is stated in document.

- Information System Security Regulations
End user E thinks that he remembers Information System Security Regulations, he could recall that there are described all password requirements.
After viewing document, he said that it is written in difficult language as normative
document and requires additional comments to explain and activities to enforce. He also
noticed that some requirements, UPS necessity for example, are not followed by responsible
persons and that makes him to think that he also can ignore requirements. So his opinion is
that document is provided only for officials. And all control and limitations are threatening
to him.

- Training, awareness
End user E has not attended information security training, but only seminars that cover job
duties. But he remembers that received some security awareness e-mails. End user E can not
isolate the cause of his knowledge about what is allowed to do and what prohibited, because
there are various forms of receiving news - manager informs, co-workers has a discussion,
receive information by email. But he considers training as good way to gain knowledge,
because every employee need regular reminder.

- Formal process of reward and deterrence
End user E thinks that his activities are only work based and are not within the scope of
deterrence process, but afraid should be only those who intentionally negatively affect
information security, so he is not afraid of being caught. But he also considers that penalties
are more effective than reward procedure about good behavior.

- Internal security culture
End user E thinks that management cares about information security, because they monitor
all activities and react if some employee is acting improperly. His main motivation for
secure behavior is fear of penalty. He holds a view that deterrence is more effective than
rewarding procedure. Although he considers that colleague’s attitudes are similar like his, he
thinks that co-workers could be a more important threat to Organization than external
hackers, but mainly because he could not imagine why hackers should interest Organization
information.

End user E thinks that changes within Organization are not rapid, they are acceptable.

- Access limitation
End user E said that his access rights are not sufficient, so sometimes he need to ask
colleague some help. And colleagues ask him, because he has access to one necessary
external IS, so it has become a common to help each other. For end user E Internet
limitations do not seem reasonable, because it endanger internal sense of trust. Employees
are trusted to use information system, but Internet limitation show that management does not
trust employees enough. Physical access limitation with smart card also does not allow to access all rooms, and need
to ask for help.

- Passwords
End user E could recall that he needs at least 6 passwords for providing his duties. He thinks
that it is very cumbersome, because additionally everyone has personal passwords and PINs.
Main problem is that every system has various frequency of password change, different
requirements for passwords, so it is difficult to invent new password. That creates problem
for End user E and he feels terrible about password policy. Password reset procedure is easy for external systems, but local systems require phone call and it is frustrating, although IT supports attitude is nice.
• Smart cards
End user E likes smart card access system; it does not create the problem even if card is forgotten, then colleagues help to get in.

• Monitoring
End user E already get used to video surveillance, and he perceives this system to protect employees from situations when clients later deny what they said, but still he considers that video surveillance should not be used to threaten employees. Some rooms do not have surveillance so it could be used for rest. End user E has not thought about possibility that network traffic is monitored and this idea does not like.

Conclusion about end user E cognition, affect and behavior

Cognition
End user E does not know the majority of security requirements, he gained his knowledge by various ways, mainly from colleagues, and therefore the knowledge is not always appropriate.

Affect
End user E has problems with password policy, it makes him feel dissatisfied; also he feels mistrusted because of Internet limitations.

Behavior
End user E has some cognitive and emotional factors that may make him feel dissatisfied, but it should not be considered to be a serious motivation for intentional attacks. End user E has noticed that he is affected by skill level errors quite often. Other threats like errors, negligence and carelessness also increase as almost all security decisions are left to end user.
Comparing results

Interviewees are working within Organization from 3.5 to 10 years; average working time within Organization is 6.5 years. Four interviewees consider that Organization employees are not the main threat to organization information systems. Only one interviewed end user thinks that employees are a more serious internal threat and can intentionally harm information security.

There are no registered intentional security attacks performed by insider, but overall end user attitude and behavior showed that the level of internal threat caused by carelessness and negligence is high, because end users are not aware of security requirements and their behavior is not secure.

The majority of end users consider it almost impossible to make an unintentional error that could impact information security; all errors are minimized within system level or business process level. Only one interviewee noticed that it is easy to make a mistake, because of few occasional tasks among routine tasks, which means – skill level errors are applicable.

Table 6-1 shows the main feelings and knowledge of all interviewees in a simplified form; more detailed descriptions are available below. As internal culture can not be assessed by end users, it is not included in this table.

Table 6-1 Comparison of cognition and affect about countermeasures

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>No opinion (does not remember)</td>
<td>No opinion (does not remember)</td>
<td>No opinion (does not remember)</td>
<td>No opinion (does not remember)</td>
<td>No opinion (does not remember)</td>
</tr>
<tr>
<td>agreement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS Security</td>
<td>Remember document, not requirements</td>
<td>No opinion (does not remember)</td>
<td>No opinion (does not remember)</td>
<td>Remember document, not requirements</td>
<td>Remember only password requirement.</td>
</tr>
<tr>
<td>regulations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training,</td>
<td>Has not attended</td>
<td>Has not attended</td>
<td>Has not attended</td>
<td>Has not attended</td>
<td>Has not attended</td>
</tr>
<tr>
<td>awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reward,</td>
<td>Deterrence is effective</td>
<td>Deterrence – neutral</td>
<td>Deterrence is effective</td>
<td>Deterrence – neutral</td>
<td>Deterrence is effective</td>
</tr>
<tr>
<td>deterrence</td>
<td>Reward is not effective</td>
<td>Reward – neutral</td>
<td>Reward – neutral</td>
<td>Reward is not effective</td>
<td>Reward is not effective</td>
</tr>
<tr>
<td>Access control</td>
<td>IS – neutral</td>
<td>IS – neutral</td>
<td>IS – negative</td>
<td>IS – positive</td>
<td>IS – neutral</td>
</tr>
<tr>
<td></td>
<td>Internet – neutral</td>
<td>Internet – negative</td>
<td>Internet – negative</td>
<td>Internet – negative</td>
<td>Internet – neutral</td>
</tr>
<tr>
<td>Authentication</td>
<td>Neutral</td>
<td>Neutral</td>
<td>Negative</td>
<td>Negative</td>
<td>Negative</td>
</tr>
<tr>
<td>based on</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

59
<table>
<thead>
<tr>
<th>passwords</th>
<th>2 passwords</th>
<th>2 passwords</th>
<th>6 passwords</th>
<th>4 passwords</th>
<th>6 passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart card usage</td>
<td>Positive</td>
<td>Positive</td>
<td>Positive</td>
<td>Positive</td>
<td>Positive</td>
</tr>
<tr>
<td>Logical monitoring</td>
<td>Neutral</td>
<td>Neutral</td>
<td>Neutral</td>
<td>Negative</td>
<td>No opinion</td>
</tr>
<tr>
<td>Video surveillance</td>
<td>Neutral</td>
<td>Positive</td>
<td>Positive</td>
<td>Negative</td>
<td>Positive</td>
</tr>
</tbody>
</table>

**Confidentiality agreement**

Confidentiality agreement was signed during employment process or, if employee was working before year 2003 when the document was approved by the management, in year 2003.

Two interviewees said that they remember the fact of signing; one end user signed it 6 years ago, other 7 years ago. No one of interviewees remembers what was stated in Confidentiality agreement.

Bet overall interview and observations during interview showed that end users have knowledge about most important statements within Confidentiality agreement.

**Information System Security regulations**

As end users do not know about documented norms, they do not influence employee behavior and therefore internal threat, except for giving a misleading security feeling to those responsible. The majority of interviewees admitted that they do not know what is stated in Information System Security Regulations. Everyone knew only the requirement for password changing.

Another issue that was pointed out was that too much information (instructions, procedures, regulations, policies) can lead to a situation where employees are not able to remember them, especially if norms within the document are not reminded regularly as Frank et al (1991) state, and management does not show their importance. Password policy proves that, because employees are reminded to change password, therefore they knew about that requirement.

At the final part of interview this document was shown to employees and they were asked to express their feelings about it. Observations were gained during their browsing of the document - end users were unpleasantly surprised about the strict security requirements that they turned out to be actually violating every day.

Some end users mentioned that there are too many restrictions, they are threatening and make them feel as a “criminal”, which means the risk of losing trust. Besides, all end users said that the document is very difficult to perceive, so it is against the Cappelli et al (2009b) recommendation that policies should be clear.

**Training and awareness**

Not a single one of the interviewees has attended information security related trainings and they could remember very few awareness-raising activities, mainly in the form of e-mail.
The majority of end users think that training is a valuable way of gathering knowledge and there should be annual trainings on information security issues.

**Reward and deterrence process**
Three end users consider that their security behavior is improved by fear from being caught and receiving a penalty. Two others think that there is no need to fear because their behavior is good.

Only one end user mentioned that reward process is an effective way to improve security behavior, and he was also the only one from interviewees who has been rewarded.

**Internal culture**
All interviewees emphasized the importance of team work and need to assist each other, it is acceptable for them. Only a few expressed the opinion that co-worker requests for help are sometimes inconvenient. As the majority of end users said that they are afraid of being caught after unacceptable action and afraid of penalty, then by using other colleagues' trust or authentication credentials, a malicious employee could use a colleague's identity and reduce the possibility of being caught, thus increasing internal threat level.

All interviewees express their satisfaction with working conditions and environment within Organization. One of the major causes for employee satisfaction is that unemployment rate in the country is high and Organization provides a stable job with at least a guaranteed salary. So motives for appropriate behavior are mainly based on fear of losing a stable job.

Interview analysis showed that fear from penalty and possibility of getting caught still is quite an effective way for reducing internal threat.

Organization internal security culture is not positively influenced by the management or the person responsible for information security.

**Access control**
Physical access right limitations are perceived as measures for the protection of employees' belongings, they are easy to use, so end users perceive them positively and not as a bother. Even when they can not access some premises that are not available for them because of confidential information, they expressed understanding.

IS access right limitations are not perfectly based on need, so some inconvenience is appearing as colleague help is needed or colleagues are asking for help. But only two end users reported that it is cumbersome.

End users do not consider that there is need to limit Internet access and some of them even noticed that there is trend of using other proxy servers. Four persons think that work performance is not affected by internet limitations, and only one end user expressed an opinion that his colleagues do not need Internet at all.

**Passwords**
End users have a different number of passwords necessary, two employees said that they
need 2 passwords, one needs 4 passwords and two need 6 passwords. Those who need 2 passwords do not report problems with creating and remembering them.

Employees who need more than 4 passwords indicated that they are using external information systems with more restrictive password policy, so those who need 4 and 6 passwords said that it is too difficult to create and remember the passwords. But internal systems are not the ones who create password problems, because no complexity requirements are set.

All interviewees were dissatisfied with situation that IS does not automatically request password changing, but end users must remember themselves to change them.

Smart cards
All interviewees expressed their positive attitude to smart card system as a physical access limitation. They were positively minded because the system is easy usable, does not require to enter PIN and provides protection for their belongings.

But it should be noted that this smart card authentication system is not so effective in preventing internal threat because no clear policy of use is documented, and employees are used to borrowing each other's cards and can access all premises anyway.

Monitoring
All interviewees hold a view that employees have privacy rights within Organization, some of them feel that Organization provides enough privacy, but others feel that they do not have privacy, mainly because of strong video surveillance control.

One of the Organization’s focuses is to improve client service, so to provide that video surveillance systems have been implemented a few years ago, but now some end users noticed the tendency to use the system so that employees feel humiliated. Although some interviewees propagated the idea that video surveillance is for protecting them, others consider it to invade on their privacy and proved the discovery by Witty (2004) Irving et al (1986) that video surveillance within work place may strengthen employees' feeling of distrust and rise disgruntlement.

IS usage monitoring was understood the most positively; because it is related to job duties and everyone consider that Organization has rights to control activities within IS. Internet usage monitoring was not so positively perceived because of privacy.

6.5. Countermeasure negative influence
As noted previously, information security training and awareness process is lacking, and employees' security behavior is based mainly on what they see and their personal experience. They are not aware of security requirements within Organization, which means:

- Some security requirements are in skill level, end users know what is allowed to do in system and what is not, although they do not remember the source where these requirements were set.
- The only requirement that all interviewees remembered was the need to
change password regularly, but it is required to perform regularly and employees are aware that it is possible to automate this process,

- Password complexity requirements are set very strong in IS Security regulations, but not enforced by technical means, therefore left to employees' own sense of security, but mainly employees do not choose strong passwords, they write them down or even completely remove authentication for systems that is possible.

- Internet is used for personal use, although prohibited by IS Security Regulations. Employees have misperceived that it is allowed to browse all available sites, because of that few websites are prohibited.

Within user perception analysis the countermeasures that have negative influence on internal threat level were identified and assessed. The following countermeasures have the most negative impact on end users' security behavior and therefore can increase internal threat level within Organization:

1. Internal culture – now internal threat is most negatively influenced by unsecure internal culture. Employees are not trained or aware about proper secure behavior, so they copy colleagues' behavior and it is not always the best, for example, access right sharing, password writing.

2. Video surveillance – the trend to use video surveillance not only for post-incident or conflict situation analysis but also analyzing every word and gesture for finding mistakes in communication with clients seriously influences employee sense of privacy. It may increase motivation by revenge, disgruntlement, dissatisfaction with management and policies.

3. Authentication – 3 interviewees have problems with password remembering, so some cases of unacceptable behavior were identified: passwords are written down on paper. That increases the opportunity to get and use other colleagues' authentication credentials to use for intentional attack against information security. Additionally, as password security requirements are not implemented by technological means, end users ignore them.

4. IS access limitations – as access limitations are too strict and not adjusted according to duties, the limitations have a negative impact on security behavior. First of all, employees are used to share their access rights to fulfill their duties, to help colleagues. Secondly, accountability of performed actions is lost. And finally, it could be annoying and increase dissatisfaction if too much disturbance from colleagues is experienced.

5. Internet limitations and monitoring – the majority of end users perceive Internet restrictions negatively, they feel that employer does not trust them and it raises lack of understanding about trust within Organization and disgruntlement about not being able to access some websites even when some free time from clients or other work duties.
7. CONCLUSION

The first part of this chapter contains conclusions that were achieved based on literature and empirical data analysis. The second part of this chapter contains future research suggestions.

7.1 Conclusion

The aim of this study is to gain better understanding about human perception and how information security countermeasures influence human behavior. The research question was “How information security countermeasures are perceived by employees and how they change their behavior affecting internal threat level”. Case study methodology was applied to research on this question.

The overall conclusion is that security countermeasure acceptance and employee satisfaction are very important to ensure secure behavior, but interview analysis showed that end users perceive countermeasures differently, although there are some common signs that are described within the conclusion.

Internal security related documents were very complex and difficult to understand, awareness processes were not established to refresh knowledge, technological countermeasures were not implemented to make following requirements easier and internal security culture was not influenced for better security behavior. Documentation analysis, interviews and observations showed that the person responsible for information security is not aware of the internal threat importance, human factor and that human factor influences internal threat level as it was identified as one of the SME information security characteristics.

The results of the empirical study showed four main conclusions:

Firstly – information security related documentation does not affect employee behavior if regular reminders and awareness are missing or if employees see that others do not follow security requirements. End users read, sign and forget; therefore formal documentation could be of use only in the case of a conflict situation. That means – if employees are not aware of security requirements that are set by the organization, their behavior is based on experience and the behavior of other co-workers.

Secondly – informal norms have a serious impact on each employee security behavior, especially if formal norms are not implemented appropriately. Employer and colleague attitude and everyday security behavior, trust that is established among employees, co-worker duties and social interaction are examples of factors that influence end user decision taking regarding information security.

Thirdly – there are technological countermeasures that may negatively influence employee behavior and raise information security threat level. Authentication, access control and monitoring were analyzed to identify how end users perceive them. End users who need more than 4 passwords reported cognitive problems for creating and remembering them. Internal access limitations are not efficient if they are not adjusted according to the duties and an internal culture with access right sharing is spread. Monitoring can seriously affect employee satisfaction and therefore motivation for internal threat.

And finally, end users most positively perceive countermeasures that are implemented with a clear message about how they could give benefit for end users. Even such a privacy invasive
technology like video surveillance was accepted by half of interviewees because they saw the benefit – possibility to later disprove wrongful accusations by clients.

Analysis of end user security behavior showed that the possibility for error affecting information security is reduced by system design, separation of duties. Employees are satisfied by work stability and are afraid of being fired; therefore their motives for intentional attack are reduced. Analysis showed that internal threat caused by employee negligence, carelessness and cognitive based errors are the most important issues that should be addressed, because employees are not trained or aware about what is a good security behavior, they merely adopt co-workers attitude and behavior.

It should be concluded that overall organization culture, environment and other external factors are so important that there is no single perfect formula for improving good behavior that could be adopted for every organization.

To improve information security, each organization must assess their employee attitude toward various security issues, explain to employees the need for countermeasures and the benefits for employees, and only then implement and maintain countermeasures.

### 7.2 Future research

The area of human factor within information security is still not fully explored and needs further investigations, although within the past few years there has been a great emphasis on researching social psychology, cognitive science, and neuroscience from the point of information security risks. The interaction between information security and human psychology will be the big research area within the next years (Anderson, 2008), so not only knowledge about how security countermeasures for internal threat are perceived should be researched, but any interaction among security and psychology will help to improve information security.

This thesis researched one organization and its countermeasures and end user perceptions, therefore there is the risk of result generalizations, so more case studies and comparison of results would deliver more precise conclusions.

This thesis contains descriptions of various effects on end user security behavior that can raise countermeasures, and there is no emphasis on recommendations how to improve security behavior; developing detailed recommendations requires additional research.

Some other security countermeasures that were not used within case study Organization also should be analyzed, for example, procedures and instructions, single sign on, various biometrical authentication techniques, identity management systems, encryption, back-ups.

Within this thesis case study methodology was used, but other research methodologies may show the issue of human factor within information security from the different angle and reduce the impact of human bias.

In this research only some security countermeasures were analyzed from the point of end-user perception. Future researches could explore also not only the end-user, but also how security countermeasures are perceived by privileged persons – IT personnel, managers, those responsible for information security, and how they take the decisions for implementing and maintaining information security countermeasure.

As informal norms have the most significant impact on employee behavior, another field for future researches is how to influence internal security culture to improve security behavior.
REFERENCES


Schein, E (2004), Organizational culture and leadership, Willey & Sons Inc, San Francisco.


Tavris, C & Aronson, E (2007), Mistakes were made (but not by me), Harcourt, Florida.


Whitman, ME & Mattord, HJ (2008), Management of information security, Course Technology, Boston.

Whitty, MT (2004), “Should filtering software be utilised in the workplace. Australian


Yin, RK (2003), Case study research design and methods, Sage Publications, London.