Eeva Eskelinen

FACTORS AFFECTING INFORMATION SECURITY BEHAVIOR OF EMPLOYEES: A CASE STUDY

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2019

ABSTRACT

Eskelinen, Eeva
Factors affecting information security behavior of employees: a case study
Jyväskylä: University of Jyväskylä, 2019, 85 pp.
Information System's Science, Master's Thesis
Supervisor(s): Soliman, Wael

Employees can have a significant impact on the information security of organizations and to ensure secure behavior many organizations have applied information security policies. However, despite having policies in place many employees are not complying with them, thus exposing the organization to several security threats. This Master's Thesis aims in identifying factors which motivate employees to comply with their organization's information security polices and on the other hand, how they justify their non-compliant security behavior. This thesis observes these phenomena with the following research questions: *Which factors motivates employees to comply with information security policies?"* and "*How employees justify their non-compliant ISP behavior?"*. This thesis consists of a literature review and an empirical research study which was conducted as a qualitative case study. The data for this study was gathered by conducting semi-structured interviews in an organization operating in B2B. These research questions were observed through three themes which the employees' perception of their security compliance versus their actual security behavior were, motivation for compliance and justification strategies to justify non-compliant behavior. The results of the study show that the main motivators for compliance were obligation towards employer and the will to protect those individuals whose information the organization handles. For the second research question, the results suggest that the main strategies to justify non-compliant behavior were denying responsibility or injury, inconvenience, perception of risk and trust towards colleagues. The findings of the study indicate the need for educating employees about the possible risks and consequences of non-compliant security behavior, but also identifies the factors which can be used to support employees' motivation towards compliance.

Keywords: ISP compliance, security behavior, security compliance, insider threat

TIIVISTELMÄ

Eskelinen, Eeva
Tapaustutkimus työntekijöiden tietoturvakäyttäytymiseen vaikuttavista tekijöistä
Jyväskylä: Jyväskylän Yliopisto, 2019, 85 s.
Tietojärjestelmätiede, Pro Gradu -tutkielma
Ohjaaja(t): Soliman, Wael

Työntekijöillä voi olla merkittävä vaikutus organisaation tietoturvalle ja monet organisaatiot ovat ottaneet käyttöön tietoturvakäytänteitä tietoturvallisen käyttäytymisen varmistamiseksi. Yhteisistä käytänteistä huolimatta monet työntekijät eivät noudata tietoturvaohjeistuksia ja siten altistavat organisaation monille tietoturvauhkille. Tässä Pro Gradu -tutkielmassa pyritään tunnistaman tekijöitä, joita työntekijät kokevan motivoivan heitä noudattamaan organisaationsa tietoturvakäytäntöjä ja toisaalta tunnistamaan menetelmiä, joilla työntekijät perustelevat tietoturvakäytäntöjen vastaista käyttäytymistä. Tämä tutkielma tarkastelee ilmiötä seuraavilla tutkimuskysymyksillä: *"Mitkä tekijät motivoivat työntekijöitä noudattamaan tietoturvakäytäntöjä?"* sekä *"Kuinka työntekijät perustelevat tietoturvakäytäntöjen vastaista käyttäytymistä?"*. Tämä tutkielma koostuu kirjallisuuskatsauksesta ja empiirisestä tutkimuksesta. Tutkimuksen aineisto on kerätty toteuttamalla semistrukturoituja haastatteluja yrityksessä, joka toimii B2B-sektorilla. Tutkimuskysymyksiä tarkasteltiin kolmen eri teemaan avulla, joita olivat seuraavat: työntekijöiden käsitys omasta tietoturvakäyttäytymisestään ja sen vertailu todelliseen tietoturvakäyttäytymiseen, työntekijöiden motivaatiotekijät tieto-turvakäytäntöjen noudattamiseen sekä strategiat, joilla työntekijät perustelivat käytäntöjen vastaista toimintaa. Tutkimuksen tulokset osoittivat, että merkittävimmät motivaatiotekijät olivat velvollisuudentunto työnantajaa kohtaan, sekä halu suojata niitä yksilöitä, joiden henkilötietoja yritys käsittelee. Toisen tutkimuskysymyksen osalta tutkimuksen tulokset osoittivat, että menetelmät, joita käytettiin eniten perustelemaan käytäntöjen vastaista toimintaa, olivat vastuun ja vahingon kieltäminen, hankaluus, käsitys riskistä ja luottamus kollegoihin. Tutkimuksen tulokset osoittavat tarpeen työntekijöiden kouluttamiseen mahdollisista riskeistä sekä seurauksista, joita käytäntöjen noudattamatta jättäminen voi aiheuttaa. Tutkimuksessa myös tunnistettiin tekijöitä, joita voidaan hyödyntää työntekijöiden motivoimisessa tietoturvalliseen käyttäytymiseen.

Avainsanat: Tietoturvakäytäntöjen noudattaminen, tietoturvakäyttäytyminen, sisäinen uhka

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Utilizing technology and digital solutions has become vital condition for most companies and the amount of organizations completely relying on technology is proliferate. (Stanton, Stam, Mastrangelo & Jolton, 2005) To ensure technology reliant businesses to operate without disruption, information security needs to be considered. (Von Solms & Van Niekerk, 2013) In many studies, human has been considered to be the weakest link for information security and the cause for many security incidents. (Vroom & Von Solms, 2004) In organizational context, this argument applies for the employees of the organization. To ensure the quality of information security, many organizations have applied information security policies. (Höne & Eloff, 2002) However, even if policies are introduced and compliance is required, many employees are not complying with the security policies. (Siponen & Vance, 2010) Greitzer et al. (2008) argue that past and present employees of the organization form the biggest threat for the organization. Thus, the security behavior of employees has been widely studied.

One of the main concepts regarding human security behavior and especially the employees' security behavior is the concept of insider threat. Insider is someone who has or has had legitimate digital or physical access to the organization's information assets (Jouini, Rabai & Aissa, 2014). Insider threat occurs when an insider intentionally or non-intentionally violates the organization's security policies and causes security threats for the organization. (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005) Therefore, the employees' behavior regarding the security policies is an interesting topic for a study. In this paper, the employees' motivation to comply with security policies are studied to better understand how employees can be encouraged to act compliantly. Another point of view studied in this paper is the strategies with which the employees justify their non-compliant behavior. With these findings the organizations can tackle the factors which are preventing or not motivating the employees to act compliantly. Thus, the research questions for this study are the following: "*What motivates employees to comply with information security policies?*" and *How employees justify their non-compliant ISP behavior*". Next, the method of conducting this study is presented.

These two research questions are studied by conducting a literature review and an empirical research study. The literature review aims in creating understanding of the existing literature regarding security behavior of employees. The literature review was conducted based on the framework of conducting a systematic literature review by Okoli and Schabram (2010). The most utilized tool for searching literature for this study was Google Scholar. To find relevant studies, the following words and their combinations were used: information security, security behavior, insider threat, non-malicious security behavior, employees' security behavior, information security policies, information security policy compliance. As behavioral theories extend to psychology and social studies, some limitations regarding these theories were made. For this study, only studies related to information security behavior are included and other behavioral theories are excluded from the scope of this study.

The empirical study was conducted as a qualitative single case study. The researched data was gathered by conducting semi-structured interviews in a Finnish organization operating in B2B business. Nine employees of the organization were interviewed. The interviews were transcribed word-to-word and coded based on three identified themes. The themes were the following: the employees' perception of their security compliance versus their actual security behavior, motivation for compliance and justification strategies to justify non-compliant behavior. The interviews were analyzed using thematic content analysis.

In this study, the research questions are observed and analyzed based on the findings of the literature review, including different behavioral theories, which have been used to explain employee security behavior. The findings of the empirical study regarding the first research question about the motivational factors differed from the findings of the literature review, although some similarities were identified, as well. The study suggests that the main motivational factors were related to obligation towards the employer, including protecting the business and its reputation, protecting organization's customers and the fear of legal consequences. Regarding the second research question about the justification strategies, it was observed that almost all strategies identified in the literature review were identified in the empirical study, as well. Other strategies were also observed, which were not identified in the literature review. The main strategies identified were denying responsibility or injury, inconvenience and perception of risk.

This thesis consists of the introduction chapter and six main chapters. The contents of the thesis are structured as follows. In the second chapter, the main concepts of this study are defined, including insider threat, malicious and non-malicious security behavior and a classification of security threats. In the third chapter, the relevant theories regarding security behavior identified from the literature are introduced and discussed. The fourth chapter summarizes the literature review. In the fifth chapter, the research method and scope for the empirical study are introduced. This chapter presents the research and data acquisition methods, the case organization and the process of conducting the study.

In the sixth chapter, the results of empirical study are presented. In the seventh chapter, the results of the study are discussed and analyzed. Also, the limitations of the study and suggestions for further study are discussed. The eighth and final chapter of this paper concludes this study.

2 INFORMATION SECURITY

Information technology has taken an increasing role in many organizations' business operations, as it has become more essential part of many people's every-day personal life, as well. The amount of business operations which are not relying on technological solutions have been decreasing substantially. (Stanton et al. 2005) It goes without saying that utilizing technology has its benefits, but technology does not come without its challenges, especially regarding security. Maintaining security requires complex solutions, including technical and socio-organizational solutions.

In this chapter, the relevant concepts regarding this study are introduced. In chapter 2.1 the definition of information security is discussed. The classification of information security threats is presented and the threats relevant to this study are defined. In 2.1.4 the difference between malicious and non-malicious behavior is defined. In chapter 2.1.5 the possible security violations are discussed. As chapter 2.1 focuses on defining the scope of this study, chapter 2.2. focuses on the possible solutions for security violations. In chapter 2.2.1 information security policies are introduced and in 2.2.2. information security strategy is discussed. In 2.2.3 the definition of security compliance is introduced and finally, in chapter 2.2.4 the previous literature is presented.

2.1 Relevant concepts

In this subchapter, the relevant concepts regarding this study are defined. This chapter focuses on limiting and defining the scope of this study.

2.1.1 Defining information security

Despite its common useinformation security has multiple definitions and there seems to be no unified definition in the literature. The terms information security, cyber security and information and communication technology (ICT) are

often mixed up or used inconsistently. However, the term information security is generally defined by the so-called CIA triad. Based on CIA triad, the aim for information security is to preserve the confidentiality, integrity and availability of information. (Farooq et al. 2015; Theoharidou et al. 2005; von Solms & von Niekerk, 2013) Confidentiality refers to the ability to provide privacy and protection to users' or data owner's sensitive information. Protecting the integrity of information refers to the actions which are made to ensure that the sensitive information cannot be modified without the data owner's acknowledgment. Availability refers to the ability to access sensitive and critical information immediately any time necessary. (Farooq et al. 2015)

ICT security aims in protecting the confidentiality, integrity and availability of information resources, but also to protect the non-repudiation, accountability, authenticity and reliability of information resources. (von Solms & van Niekerk, 2013) Non-repudiation ensures that the actions of an individual cannot be denied afterward, meaning that actions can be traced back to the individual who has carried them out. Non-disclosure ensures that information is available only to individuals who have the required authorization for it. (Siponen & Oinas-Kukkonen, 2007) Information systems security, on the other hand, is a wider concept, which aims in protecting all elements information systems consists of, including hardware, information, people (users, administrators etc.) and so forth. In other words, information systems security refers to all the parts that are included in the functions of information systems, including the users and the administrators as well as the technical hardware. (Theoharidou et al. 2015) Therefore, it could be said that the focus of this study is on information systems study, as the interest is in the people. However, information security is a stabilized term to describe security as a wide concept. Therefore, the term information security will be mostly used in this paper.

2.1.2 Classification of security threats

To create adequate information security policies, potential security threats need to be recognized and evaluated. By recognizing the possible security threats, organizations are more able to protect themselves against them. (Jouini et al. 2014) Loch, Carr and Warkentin (1992) present a four-dimensional model of information systems security (Figure 1) which demonstrates the various security threats. Based on the model, security threats consist of the sources, perpetrators, intent and consequences of security threats. The model divides the sources of threat into internal and external threats. Perpetrators can be either human or non-human. The intent of the threat can be either accidental or intentional. The consequences of security threats are divided into disclosure, modification, destruction and denial of use. (Loch et al. 1992) Disclosure means a situation, where the organization's assets or information is exposed or leaked. Modification means the organization's data is modified without the knowledge of the administrators. Destruction means the data is being destroyed. Denial of

use means that the access to the system or data is being prevented. (Loch et al. 1992)

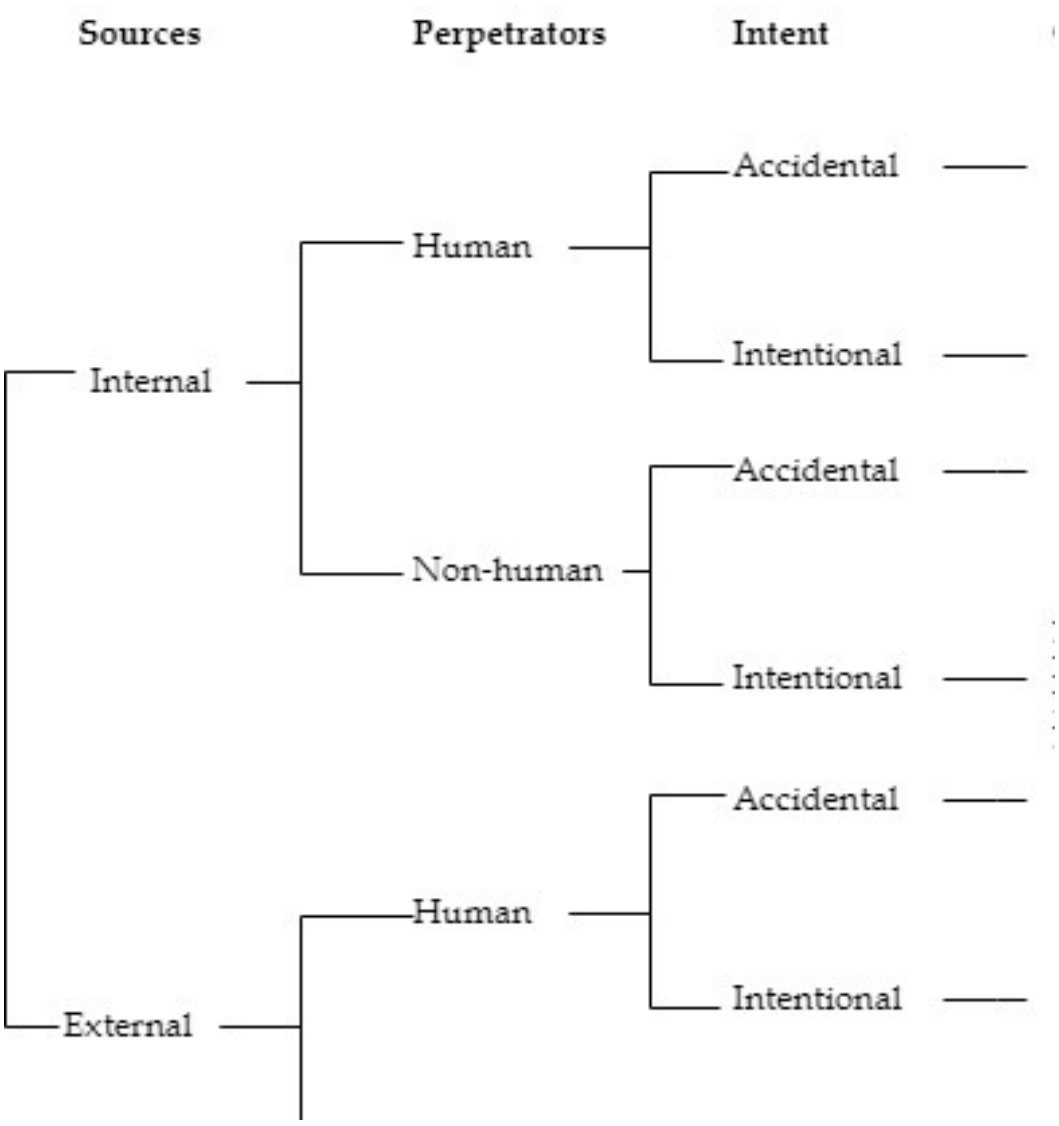

Figure 1 – Classification of security threats. (Modified from Loch et al. (1992)

The model by Loch et al. (1992) has since been modified and extended by Jouini et al. (2014) (Figure 2.) The model has many similarities, but some parts from Loch et al.'s model have been extended. Similar to Loch et al.'s (1992) model, Jouini et al. (2014) have divided the sources of security threats into external and internal threats. The threats are caused by so-called threat agents, which can be human, environmental or technological. Environmental and technological threat agents' motivation can be only non-malicious, as they are always a result of an accident. Human threat agents' threat motivations, on the other hand, are divided into malicious and non-malicious, and the threats can be caused either accidentally or intentionally. Regardless of the intention of the threat, the impacts are same in every situation. The impacts can be destruction of information, corruption of information, theft or loss of information, disclosure of information, denial of use, elevation of privilege and illegal usage. (Jouini et al. 2014) The concepts of insider threat, malicious threats and non-malicious threats will be further discussed in the next chapter.

Jouini et al.'s (2014) model also shows seven different threat impacts. The security threats can cause one or more impacts to the organization's systems or network. The seven threat impacts are:

1. Destruction of information
2. Corruption of information
3. Theft or loss of information
4. Disclosure of information
5. Denial of use
6. Elevation of privilege
7. Illegal use

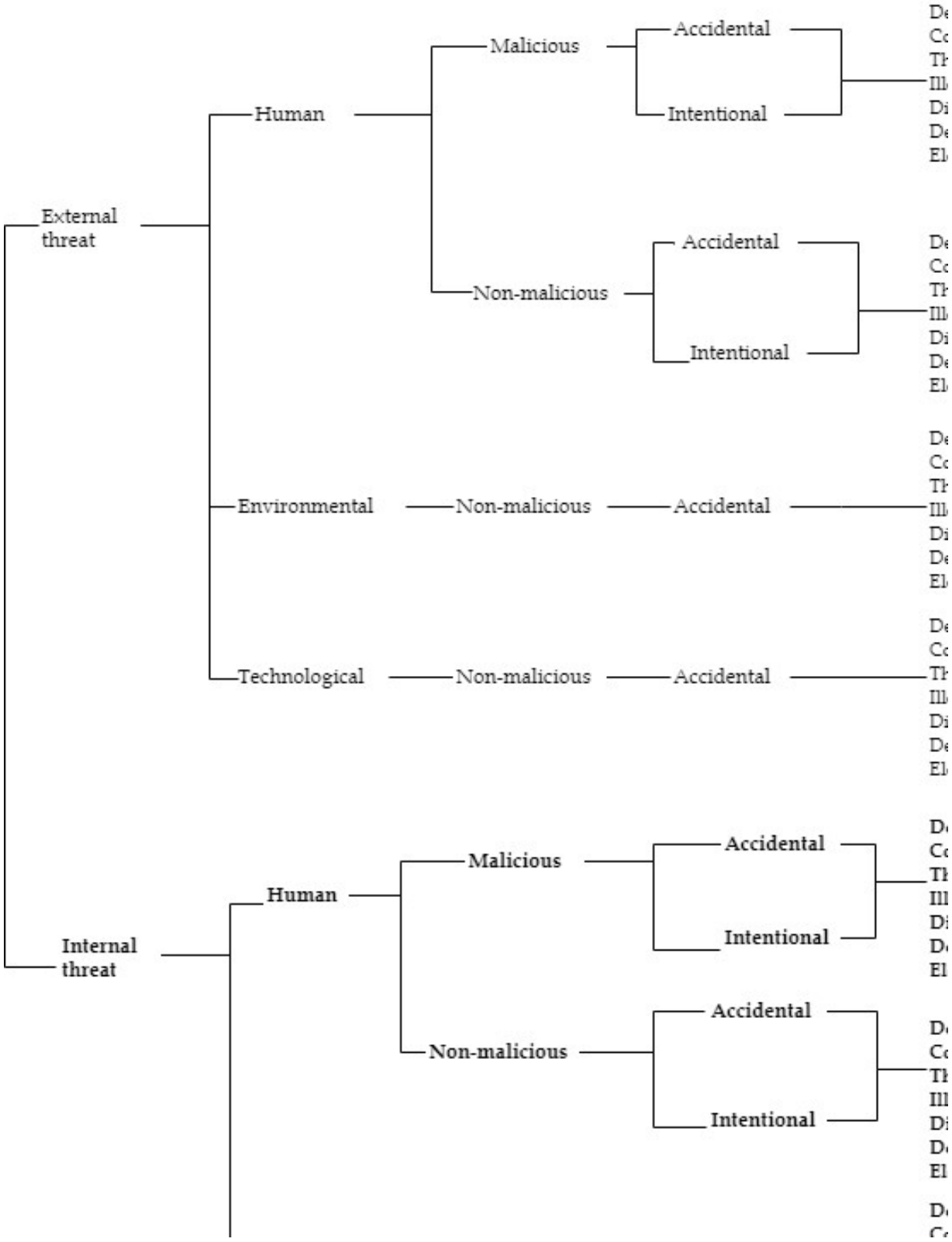

Figure 2 – Classification of security threats. Modified from Jouini et al. (2014)

Farahmand, Navathe, Sharp and Enslow (2005) propose a slightly similar model for threat classifications and control measures (Figure 3.) The model

identifies three threat agents which can be unauthorized user, authorized user and environmental factor. The techniques used to cause threat are physical, personnel, hardware, software and procedural. To protect the information security threats, the model also proposes security measures which can be taken. The potential measures are authentication, access control, data confidentiality, data integrity and non-repudiation. (Farahmand et al. 2005)

The main difference between the model by Farahmand et al. (2005) and Jouini et al. (2014) is with the threat agents. The differing factor is that Farahmand et al. (2005) doesn't divide threat agents into external and internal, but into unauthorized users and authorized users. This division is supported by the theory by Schultz (2002), who discusses the difficulty to define, who counts as an insider and who does not. Therefore, it makes sense to divide the threat agent into those who have legitimate access to the IS assets and those who have not. Authorized users can become threats if they make errors or exceed their privileges. Unauthorized users have no authorized access to the system and they intentionally interrupt or sabotage it. The environmental factors are usually considered to be natural disasters, such as floods (Farahmand et al. 2005) or power failure. (Im & Baskerville, 2005)

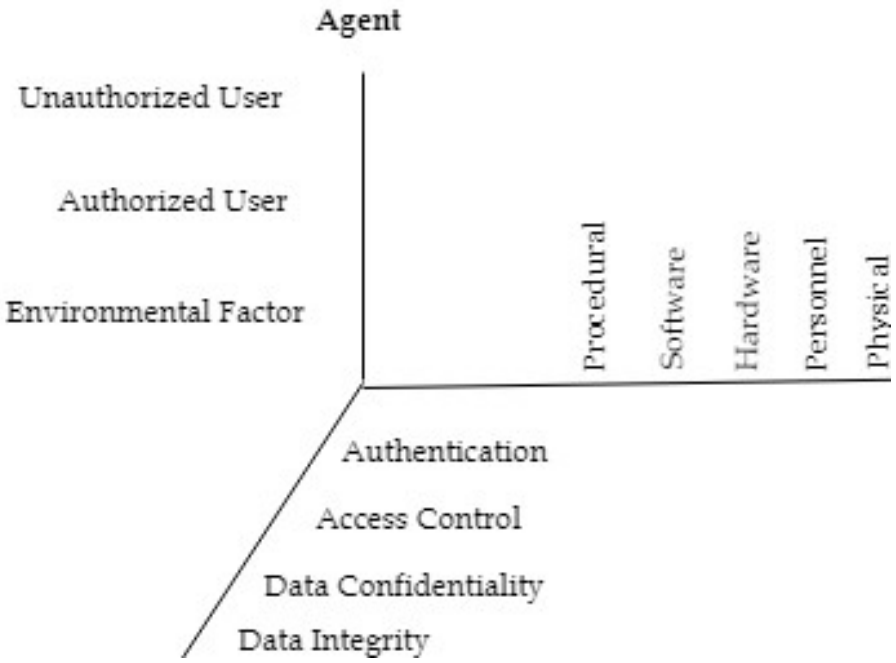

Figure 3 – Security threat classifications and control measures. Modified from Farahmand et al. (2005)

2.1.3 Insider threat

According to Greitzer et al. (2008), several surveys have shown that past or present employees are one of the biggest security threats to organizations. Thus, this study is limited to observe insider threat and more specifically, employee security behavior. Insider threats are security threats originating from the inside of the organization by current or previous employees. Insider threat can be defined as human behavior, which occurs when an individual does not comply with the organization policies with either malicious or non-malicious intentions. (Greitzer et al. 2008) Insider threats are caused by people, who have or have had authorized access to the network either with an account or by having physical access. (Jouini et al. 2014)

Insiders are often considered to be the employees of the organization, but insider can also be an external consultant, a contractor or even a former employee or former third-party consultant. (Schultz, 2002) In other words, insider threats are carried out by someone who has or has had legitimate access to the information security assets of the organization. (Leach, 2003) One factor increasing the chance of insider threats is outsourcing. With outsourcing, it can be challenging to control, who has access to the information of the organization. Therefore, outsourcing can possibly reveal the information of the organization to hundreds of people who have no legitimate access to the information. (Colwill, 2009)

Schultz (2002) also points out that it is often challenging to determine if the threats or attacks have originated from the actions of an insider or not. Sometimes it can also be challenging to determine, who is counted as an insider and who as an outsider. Many companies have outsourced contractors or consultants, who have access to the organization data. If insider threat is defined based on authorized access, an insider could, in that case, be someone from an outsourced third-party organization. The security attack can also be a result of collaboration between an insider and an outsider, which makes determining the source of the threat even more challenging. (Schultz, 2002)

Insider threats create remarkable threats to the organization as employees have the possibility to harm the confidentiality, integrity and availability of the information systems of the organization. (Warkentin & Willison, 2009) Insiders can often cause more damage to the organization than external attackers as they have legitimate access to the information and the facilities of the organization. (Colwill, 2009)

2.1.4 Malicious and non-malicious security violations

As it was defined in the previous chapter, security violations can be a result of either malicious or non-malicious behavior. Security violations are "threats against the confidentiality, integrity and availability of the information of the organization." (Workman, Bommer & Straub, 2008). Information security policy violations can be defined as "unauthorized access to data and systems, unau-

thorized copying or transferring of confidential data or selling confidential data to a third party." (Hu, Xu, Dinev & Ling, 2011) Security violations can also be defined as misuse of IS assets. IS assets can be, for example, hardware, software, data and other computer services. Misuse of such assets can be damaging the hardware, misappropriation or destruction of data, unauthorized use of devices etc. (Kankanhalli, Teo, Tan & Wei, 2003)

Another form of security violation is social engineering, which means manipulating the users to hand over their passwords, user identification or other sensitive information, which can then be used against the users themselves or the organization. (Rhee, Kim & Ryu, 2009) Although it would be easy to think that social engineering is only applied by external attackers, it is, in fact, often carried out by another employee. (Peltier, 2006) Social engineering can be considered as an easier way to violate security, as the attacker does not need hardware or hacking skills for the violation. However, social engineering often requires some knowledge of the systems and protocols of the organizations, or knowledge about the other employees of the organization to be credible. One way to protect the employees from social engineering is to educate them of the situations in which their user identification can be legitimately requested and when it cannot. (Peltier, 2006)

Malicious behavior is carried out by an individual who has access to the organization's data or network (Greitzer et al. 2008) and who intentionally violates the organization's policy by misusing his/her privileges (Theoharidou et al. 2005) Non-malicous behavior is carried out by an individual, who has no intention to harm the organization but ends up doing so by violating the organization's policies. (Warkentin & Willison, 2009)

For non-malicious behavior, Guo, Yuan, Archer and Connelly (2011) propose further characteristics. The first characteristic is intentionality, as the violation is not a result of an accident. Secondly, the violations do not aim to harm the organization. Thirdly, the employee looks for self-benefit without having malicious intentions. The authors' example of this characteristic is skipping certain policies or rules to save time. Fourth, an employee voluntarily breaks the rules or violates the organization's policies. Although the aim for these actions is not to cause harm to the organization, the employee can cause damage or expose the organization to several security threats. (Guo et al. 2011) An example of non-malicious behavior could be forgetting to change passwords, forgetting to log out of the computer when leaving the workstation unattended, (Greitzer et al. 2008; Warkentin & Willison, 2009) sharing user identification and passwords with colleagues and failing to make regular backups. (Pattinson & Anderson, 2007) It has been argued, that non-malicious security behavior is often a result of weakly implemented information security policies. (Jouini et al. 2014) Even if the violations have been made with no malicious intentions in mind, they expose the organization to several security threats. Therefore, even the possibility of non-intentional security violations needs to be acknowledged and cut out. (Warkentin & Willison, 2009)

According to Greitzer et al. (2008), the objective to carry out malicious actions can be the intention to cause harm to the organization or to gain personal benefits. Insider threats caused by malicious behavior can be, for example, gaining unauthorized access to information, sabotage or negligent use of classified data. (Greitzer et al. 2008) Malicious behavior can also appear as computer abuse, where the company assets are intentionally damaged or the organization's data is modified. (Guo et al. 2013; Jouini et al. 2014)

To avoid both malicious and non-malicious behavior, there are some technical control actions which can be taken, although technical controls do not take the human factor into account. Technical controls to be taken can be encryption, access control, granting only the minimum access privileges, monitoring and auditing. Controls aimed to control employee behavior can be implementing security policies and procedures and conducting personnel checks. (Colwill, 2009) Solutions for avoiding security threats are discussed in more detail in the following chapters.

2.2 Solutions

Information security violations, especially security breaches can become costly for organizations. The costs from security breaches are often intangible and thus difficult to determine the exact amount of losses. The most visible cost of a security breach is the decrease in market value, if the breach is publicly announced. Security breaches can weaken the trust of both customers and investors as they might question the reliability of the organization, thus possibly creating financial losses. (Cavusoglu, Cavusoglu & Raghunathan, 2004)

As security violations can cause significant harm to the organization, many solutions can be applied to avoid security violations. In this subchapter, the different types of solutions are presented and discussed. In chapter 2.2.1 Information security policies are introduced. Chapter 2.2.2 focuses on defining compliance in a security context. Chapter 2.2.3 introduces the previous literature regarding the topic.

2.2.1 Information security policies

As protecting organizations' IS assets is crucial for ensuring the continuity of business operations, different kinds of actions can be taken in place. To maintain the expected level of information security, most organizations have applied information security policies (ISP's) (Höne & Eloff, 2002). Bulgurcu, Cavusoglu and Benbasat (2010, p.526) define ISP's as "a statement of roles and responsibilities of the employees to safeguard the information and technology resources of their organizations." International security standard, ISO 27001, states that ISP's "provide management direction and support for information

security in accordance with business requirements and relevant laws and regulations." (Disterer, 2013, p. 96) ISP's usually should cover all business operations of the organization, as well as all security measures from technical solutions to organizational awareness of risks and threats. (Höne & Eloff, 2002)

The increasing use and need of information systems indicates that in most companies, all employees have access to (at least some parts of) the company information either digitally or physically. Since all employees are not experts in information technology or information security, organizations need to apply security policies and educate their employees about the contents of the policies to help them ensure the protection of the organization's information security and critical information. (Thomson & von Solms, 1998) As organizations can be in possession of great amounts of sensitive information, there is a need to protect the information assets of the organization. However, just as importantly, the legislative requirements need to be considered, as well. (Hsu, 2009) One of the recent legislative regarding data protection requirements for organizations in EU is the General Data Protection Regulation, GDPR, which is discussed further later in this paper.

There are international standards for information security and ISP's which can help organizations create their policies, but they do not give direct instructions or guidelines on what should be included in the policies. Höne and Eloff (2002) highlight that all ISP's should be tailored for each organization and the organization itself should consider the needed parts for the policy, rather than blindly following the instructions of the general standards.

Although the ISP's are recommended to be tailored for each organization's needs, there are common elements which are usually covered in every ISP. Höne and Eloff (2002) have identified in their research, that ISP's often include the following:

- Need and scope for information security
- Objectives and definition of information security
- Management commitment to information security
- Purpose of the security policy
- Information security principles
- Roles and responsibilities
- ISP violations and disciplinary action
- Monitoring and review
- User declaration and acknowledgment

ISP's can provide extensive assistance to the top management of the organization. Siponen and Oinas-Kukkonen (2007) conducted a survey to existing information security literature and identified four security issues which had been most often discussed and studied. The identified security issues were: access to information systems, secure communication, security management and development of secure information systems.

Firstly, access to information systems includes access management, meaning the actions taken to administer who can access (and how they can access)

the organization's IS assets. An example of a method to maintain access management is limiting access rights and using different kinds of user identification methods. Second, secure communication includes the methods which aim to enable secure communication between employees or between employees and the clients of the organization. An example of secure communication is secure email. Third, security management includes planning, evaluating and implementation of security activities. Fourth, development of secure information systems aims in forming requirements for information security and aims to ensure that those requirements are met. (Siponen & Oinas-Kukkonen, 2007)

Although ISP's are expected to cover all security measures, they are generally focused on either more technical computer security measures or non-technical security management. (Baskerville & Siponen, 2002) There has been a general conception that sufficient information security can be provided by applying only technical computer security solutions. Although technical solutions can protect the organization from many threats, focusing only on the technical protection does not provide decent security as human participation has created new kinds of threats, such as phishing and social engineering. To protect the organization's information from such threats, it is important that the employees implement adequate security measures. (Aytes & Connolly, 2003) For the employees, adequate security measures should be defined in the ISP. An example of such security measure can be protecting and changing system passwords regularly. (Aytes & Connolly, 2003)

An important concept in ISP compliance is *information security awareness*. Information security awareness is a term often used to "refer to a state where users in an organization are aware of - ideally committed to - their security mission." (Siponen, 2000, p.31) Information security awareness plays an important part, as the security policies and methods are useless if the employees misuse, misconstrue or do not follow them. According to Siponen (2000) raising information security awareness minimizes user-related security faults.

According to Pahnila, Siponen and Mahmood (2007) "careless employees are a key threat to IS security". Therefore, only the existence or awareness of security policies is not enough - they also need to be complied. This brings us to the importance of the research question – it is vital to understand the factors which motivate employees to comply with security policies and on the other hand, why they choose to not comply with them.

Another complexity with ISP's is related to the diversity of possible security threats. Although ISP aims in covering all possible operations and scenarios, it cannot include advice for every situation employee might encounter with, which leaves employees to rest their actions on their best knowledge. (Leach, 2003) The challenge in constructing ISP's is that although they should thoroughly cover all operations, they should be kept short and comprehensible, so that employees would take the time to read and get familiar with them. (Boss, Kirsch, Angermeier & Shingler, 2009; Höne & Eloff, 2002; Peltier, 2006)

Another main problem in information security is that even if the organization had information security policies in place, the employees might not be fol-

lowing them. (Siponen & Vance, 2010) The changes in the way people work creates challenges for controlling the information security behavior of employees. In particular, as remote working becomes more common, the employees, who work remotely should take care of the security measures at home or wherever they choose to work. In addition to remote working, communication is in many organizations carried out via mobile applications or other channels, which increases the possible sources of security threats. (Hazari, Hargrave & Clenney, 2008). Although it is much appreciated opportunity in many organizations, remote working can create challenges for management to control the behavior of employees as compared to them working at the office.

Security controls can be used to achieve and maintain information security. Identifying necessary security controls can be challenging and expensive, but information security standards are helpful tools to do. By following the guidelines of the standards, organizations have a better ability to improve their information security. (Chang & Ho, 2006) Security standards can "be either technology-oriented or management-oriented. Technology-oriented standards deal with the physical and logical specification of a product or information technology, while management-oriented standards are designed to ensure good management practices in organizations." (Hsu, 2009, p. 141) It has been common for many organizations to rely their information security on technological solutions such as access control or firewall implementations. (Chang & Ho, 2006; Rhee, Kim & Ryu, 2009) However, ensuring the information security of the organization's assets cannot be solely achieved with technology, as the efforts of employees of the organization need to be considered as well. (Bulgurcu, Cavusoglu & Benbasat, 2010; Colwill, 2009; Gonzalez & Sawicka, 2002, October; Herath & Rao, 2009; Luo, Brody, Seazzu & Burd (2011); Posey, Roberts, Lowry, Bennett & Courtney, 2013) It has been well established in many studies that the end user's role in information security is crucial. Rhee et al. (2009, p. 816) argue that "the ultimate success of information security depends on appropriate information security practice behaviors by the end users." Accordingly, security breaches are often a result of a technical error, but an unwanted consequence of non-compliant behavior of employees. (Chan, Woon & Kankanhalli, 2008) Therefore, the organizations are advised to focus more in having employees complying with their ISP's. This thesis focuses on the employee behavior and thus, socio-organizational factors will be more closely investigated.

2.2.2 Compliance

The effectiveness of ISP's is strongly dependent on the employees' ISP compliance. Many studies have shown that employees are not often following the organizations' ISP's even if they were aware of them. (Moody, Siponen & Pahnila, 2018; Posey et al., 2013; Aytes & Connolly, 2003; Pahnila et al. 2007) The studies show that even if the required security measures were clearly defined in the ISP, the instructions are often neglected. (Aytes & Connolly, 2003) Therefore, it

is important to try to understand the reasons behind employees' security behavior.

Compliant information security behavior "refers the set of core information security activities that need to be carried out by individuals to maintain information security as defined by information security policies." (Chan et al. 2005, p. 7) The environment of the organization influences the employees' willingness to comply with the policies, but the employee also needs certain skills to be able to perform required security activities. (Chan et al. 2005)

The research by Boss et al. (2009) studied, if the perception of obligatoriness influenced the employees' attempt to take precautions against security threats. The study showed that mandatory policies do have an effect, but also that the level of specificness of the security policies had an effect, too. Therefore, the organization should focus on making the ISP detailed and understandable. Peltier (2006) also argues that the organization should focus on encouraging the employees to behave as they are allowed to do, rather than focusing on forbidding them from doing things they are not allowed to do.

An interesting finding related to security compliance was made by Stanton et al. (2005) who found in their study that the better the employees knew that their use of passwords was monitored and the more they got rewards for correct behavior, the more likely they were to change their passwords frequently and it increased the complexity of the passwords. However, it was found that complex and often changed passwords ended up written down more often. Thus, writing passwords down creates another security issue. (Stanton et al. 2005) The study is a good example of the complexities related to controlling ISP compliance and behavior – there is no simple or unambiguous solutions to the issue.

A much less studied point of view regarding employees' security behavior is how employees can improve the security of the organization. Much of the current literature is focused on the risks the employees might cause, forgetting the aspect of improving the information security. (Posey et al. 2013; Bulgurcu et al. 2010) Compliant employees can make the organization more secure, which makes security behavior such an important field of study. (Bulgurcu et al. 2010)

Workman et al. (2008) argue, that ISP compliance can be achieved by automating mandatory security measures. An example of automation is sending an automated reminder to the users to change their passwords regularly or forcing the users to change their passwords. However, automated measures are not used in every organization, for which Workman et al. (2008) have identified four reasons, which are financial, situational, cultural and technical reasons.

Financial reasons can be used as an argument if the organization does not see the threat important enough to make financial investments. Another financial argument is that some security software slow employees' computers down, thus decreasing productivity. Situational reasons can occur, for example, when the organization does not have the skills to implement automated security measures. Cultural reasons can occur if the organizational culture does not rec-

ognize security as something the individual employee should deal with. Lastly, technical restrictions can be in the way of automation, whereupon security measures cannot be completely automated. (Workman et al. 2008) From these reasons, technical restrictions are the only reason which is not related to either behavioral or cultural aspects of the organization. Financial reasons can be linked to the values and cultural environment of the organization, if the financial cuts are made due to the lack of understanding or caring about the information security. Situational and cultural reasons, on the other hand, are straightforwardly related to both cultural and behavioral factors. (Workman et al. 2008)

2.2.3 Previous literature

The reasons and motivational factors for employees' compliant and non-compliant behavior towards information security policies have been extensively studied. Studies aiming towards finding explanations for employees' noncompliant behavior are further reviewed in this chapter.

Hazari, Hargrave and Clenney (2008) studied the factors affecting work related home computer users' information security behavior and awareness. The study's focus was on the employees who work from home both full-time and part-time. The study is even more relevant today as remote working has become more common. The study showed that the factors affecting information security awareness were attitude, subjective norm and perceived behavioral control. The attitude refers to the employees' interest and motivation towards certain behavior, e.g. complying with security policies. Subjective norm is dictated by how the social pressure and learning from peers influences the employees' behavior. Perceived behavioral control refers to the level of employees' confidence towards certain behavioral performances. These factors are the basis of the Theory of Planned Behavior, which will be further discussed later in this chapter. Another finding from the study was that experience with computer-use is not related with having knowledge about information security behavior. Thus, the authors are recommending managers to regularly educate and train their employees with their security policies even if they were experienced with technology. (Hazari et al. 2008)

Another research by Leonard, Cronan and Kreie (2004) studied the factors influencing employees' intentions towards ethical behavior. The study is not directly about information security policy compliance, but it generally studies complying with the ethical protocols of an organization. The results of the study show that attitude has a significant effect on the behavioral intentions of an employee. Awareness of consequences also had significant effect on the attitude of the employee. Consequences were, in this context, either considering the outcome or actions or knowing the possibility of punishment for non-compliant behavior. Moral judgement has been shown to have positive effect in ethical decision-making and peers play a big role in that. (Leonard et al. 2004) The

threat and possibility of especially negative consequences has been widely studied in ISP literature. For example, the General Deterrence Theory implies that an individual is more likely to withdraw from committing a crime (or a security violation) if there is a possibility of severe and certain sanctions. (D'Arcy & Herath, 2011)

The research by Chan et al. (2005) studied how different factors affect the employees' perception of information security climate and how it impacts their compliant behavior. One of the findings of the study shows that co-worker socialization has considerable effect on the way employees saw the IS climate. Based on the study, employees have a significant effect on their co-worker's perception of organizations' information security climate. The results of the study align well with the arguments of the social bond theory. Chan et al. (2005) give a suggestion to the top managers to ensure that employees apply information security policies and other security practices in a daily basis in order to positively affect the state of information security and to support their peers.

Pahnila et al. (2007) studied in their research the factors affecting the employee's information security policy compliance. The authors studied the factors affecting actual information security policy compliance, the intention to comply with information security policies and attitude towards complying with the policies. Their study revealed that information quality has significant effect on actual IS security compliance. Information quality can be measured by, for example, the accuracy or clarity of the information. This means that ISP's need to be easily accessible, suitable length, the language should be understandable, and it should include relevant information to the employees. The most significant factors affecting the intention to comply with ISP found were attitude, normative beliefs and habits. Finally, the most significant factors affecting the attitude towards ISP compliance were threat appraisal and facilitating conditions. A distinctive finding from the study by Pahnila et al. (2007) was that sanctions had no significant effect on the intention to comply with the information security policies and rewards had no effect on actual ISP compliance. For example, the general deterrence theory leans mainly to the idea that the probability of sanctions would have an effect on the decisions the person makes. Pahnila et al. (2007) point out that as normative beliefs have such a big effect on the intentions to comply, the ISP compliance of top managers and peers is crucial. Therefore, if the top management emphasizes the importance of ISP compliance, it may have an effect on the intentions of other employees, too.

3 RELEVANT THEORIES

In this chapter, theories regarding IS behavior are presented and discussed. The theories introduced in this chapter were selected based on the findings from the literature review. The selected theories were appearing the most in the studies regarding IS behavior. The selection is supported by Lebek, Uffen, Neumann, Hohler & Breitner (2014) and Moody et al. (2018), who both conducted a literature review of the recently used theories regarding employees' security awareness and behavior. Most of the theories selected had been found to be the most used in their reviews. A couple of theories were eliminated from the list as they were not eligible for this study and the selection will be further discussed in chapter 3.1.

This chapter provides knowledge of the current state of IS behavior research. The theories in this chapter are used as a framework for the empirical study and the results of the study are observed from the viewpoints of these theories. It is interesting to investigate what previous research has found and to observe the extent to which these theories are applicable in a case study. The theories have been divided into individual level theories and organizational level theories. Individual level theories focus on the individual's personal motivational factors and justification techniques, organizational level theories explain, how the organization can affect the employees' motivation towards security behavior.

This chapter has been organized as follows. In chapter 3.1 the individual level theories are discussed. The theories observed in this study are the General Deterrence Theory, Protection Motivation Behavior, Social Bond Theory, Social Learning Theory, Theory of Planned Behavior, Technology Threat Avoidance Theory and Neutralization Theory. In chapter 3.2. the organizational level theories are discussed.

3.1 Individual level theories

Due to its complexity, human behavior is difficult to explain and predict. (Ajzen, 1991) However, different theories can be found in the literature regarding security behavior of employees. Lebek et al. (2014) conducted a literature review of the recently used theories explaining employees' security awareness and behavior. In their study, the theories were divided into behavioral theories and learning theories. The most used behavioral theories included the Theory of Planned Behavior (theory or reasoned action), General Deterrence Theory, Protection motivation theory and Technology Acceptance model. The learning theories included Social cognitive theory and Social Learning theory. A later study by Moody et al. (2018) also reviewed the most used theories. Most of the studied theories were the same as in the study by Lebek et al. (2014), but they also included neutralization theory, the health belief model, protection-motivation theory, the control balance theory, the theory of interpersonal behavior and theory of self-regulation.

The health belief model, the control balance theory, protection-motivation theory, the theory of interpersonal behavior and theory of self-regulation were excluded from this study as they were not appearing in other literature reviewed for this study. Also, it was important to limit the amount of theories reviewed in this study. Therefore, only the most used theories were selected. Most behavioral theories applied in IS behavior context have originated psychological or criminological theories. In this paper, the reviewed literature has been limited to IS security literature, excluding the original literature.

3.1.1 General Deterrence Theory

Deterrence theory is one of the most used theories in explaining information security behavior and it originates from criminal theories. (D'Arcy & Herath, 2011) The deterrence theory suggest that unwanted or illegal behavior can be controlled with a threat of severe and certain sanctions. The theory is based on the idea, that a person decides of committing or not committing a crime based on how low the risk is and how high the reward is. In other words, the higher the risks (e.g. punishments) are, the more likely the individual withdraws from committing the crime. (D'Arcy & Herath, 2011)

Deterrence theory has also been applied in many studies related to IS behavior. It has been studied, if employees are more likely to follow the information security policies of the organization, if the punishment of disobedience or carelessness is more severe. Hu et al. (2011) showed in their study, that deterrence, by itself, is not effective as it had no significant effect on the employees' intention to commit security policy violations. It was, however, found that by lowering the perceived benefits of security violations, it is possible to reduce malicious employee violations.

The issue with utilizing criminal theories in IS behavior studies is that ISP violations are not necessarily criminal violations, as they are often not punishable by law. (Siponen & Vance, 2010) Although deterrence theory has been one of the most studied behavioral theories regarding IS security, the results of those studies vary. Similar issue was brought up by Kankanhalli et al. (2003) is that the sanctions or penalties for IS violations or misuse are often not as severe as they might be with other crimes. However, although the results of these studies have not shown consistent results, this theory was included in this study nevertheless. As the GDPR came into effect, it was introduced in the case organization as well. It is impotysnt to observe the interviewees' thoughts of compliance regarding possible consequences. Thus, this theory was relevant to include in this study.

As another point of view, Chen, Ramamurthy and Wen (2012) studied in their research, how employees' ISP compliance behavior changes, if they were rewarded for compliant behavior. It was also studied, how combining both reward and punishment affected the employees' behavior. The results of the study suggest that organizations should, in addition to punishing for non-compliant behavior, consider having a reward system. Having a reward system may help increase employees' awareness of their ethical codes of conduct and encourage them towards more ethical and compliant behavior. (Chen et al. 2012)

3.1.2 Social bond theory

Social bond theory (also known as social control theory) also originates from criminal theories. Social bond theory suggests that strong social bonds can prevent an individual from committing a crime. Similarly, if the individual's social bonds weaken, the probability of committing a crime increases. (Theoharidou et al., 2005) According to Theoharidou et al. (2005) Hirschi (1969) defined four different types of social bonds individuals have which can prevent them from committing a crime. Those bonds are attachment, commitment, involvement and beliefs.

In this context, attachment means that individual's level of acceptance of social norms depends on the level of attachment on other people. Therefore, a person accepts social norms better if (s)he is attached to other people. Commitment means, in this context, that people who try to gain social status or reputation tend to avoid engaging in criminal activities as it might negatively affect their status. Involvement means that involvement in social activities such as clubs or hobbies decreases the time available and intention to engage in criminal activities. Beliefs means that person is more likely to engage in criminal activities if his/her belief in social norms are weak or non-existent. (Theoharidou et al. 2005)

In addition to criminals, these social bonds can be recognized in organizational context, as well. Based on Hirschi's (1969) theory, an employee is more likely to comply with organization's policies if the employee's close colleagues

or peers support compliance towards organization's policies, because the employee considers social norms important. Furthermore, if the employee looks for social acceptance or promotion in the organization, the employee is likely to be more cautious about his/her behavior. (Hirschi, 1969) It could be argued that close relationships with colleagues can prevent the employee from committing security violations, but it would require that the colleagues have a positive attitude towards policies, as well.

3.1.3 Social learning theory

The social learning theory has first been introduced by Bandura and Walters in 1977. Social learning theory suggests that "a person commits a crime because (s)he has been associated with delinquent peers, who transmit delinquent ideas, reinforce delinquency, and function as delinquent role models." (Theoharidou et al. 2005) Four different constructs have been identified to explain, how the environment of an individual affects the intention of a person to engage in criminal behavior. Those four constructs are differential association, differential reinforcement/punishment, definition of behavior and imitation. (Theoharidou et al. 2005)

Differential association can appear when an individual is faced with ethical definitions which either are in favor or against criminal behavior. Differential reinforcement/punishment refers to the expected results of criminal behavior. Expected results can be either a reward or a punishment. Definition means how an individual evaluates certain behavior. An example of evaluation can be between right or wrong behavior (Theoharidou et al. 2005) Imitation refers to the behavior an individual carries out after observing other people. (Theoharidou et al. 2005)

In the working environment, social learning theory could be seen in situations where some of the employees show clear unwillingness or indifference towards ISP's and that line of thought affects other employees as well. For example, if an employee never sees his/her colleagues locking their computer and the colleagues do not consider it to be a big deal, it can affect the employee's behavior regarding locking the computer, as well.

3.1.4 Theory of planned behavior

Theory of planned behavior originates from the theory of reasoned action. (Ajzen, 1991) A key aspect of the theory of planned behavior is "the individual's intention to perform a given behavior." (Ajzen, 1991, p. 181) In other words, the stronger the intention to perform a certain behavior, the more likely the individual is to do so. (Ajzen, 1991) Intentions can be explained with following factors: attitude towards behavior, subjective norms as social factors and perceived behavioral control. (Theoharidou et al., 2005)

Attitude towards behavior is dictated by how the individual perceives the outcome of the behavior. Positive perception results in positive attitude, nega-

tive perception results in negative attitude. Subjective norms mean that the intention to a certain behavior is affected by the attitudes and norms of the social environment of the individual. If the social environment considers certain behavior positive and the individual seeks approval from the people around him/her, the individual is more likely to behave in certain behavior. (Theoharidou et al., 2005) This aspect is very similar to the social bond theory. In organization's security context this would suggest that if the rest of the organization considers information security policy compliance to be a norm and desirable behavior, and the employee seeks for social approval, the employee is more likely to comply with the policies as well. Therefore, it would be beneficial for an organization to encourage their employees towards compliant behavior.

3.1.5 Technology threat avoidance theory

Technology threat avoidance Theory, TTAT, suggests that employee's perception of threat is based on how likely the employee considers the threat to occur and how severe the consequences of the threat would be. Based on TTAT, an employee takes actions against the threat based on the likeliness of the threat. (Liang & Xue, 2009) If the employee is unsure which security measures can be taken, the employee might deny the possibility of threat. (Liang & Xue, 2009)

The perception of risk can have a major effect on the behavior of the employee. To realise the actual risks and threats there might be, the organization should educate its employees of the possible risks it might face. The employees should also be educated on how they can protect themselves and the organization from such threats. As it was studied by Liang and Xue (2009), if the employee has no knowledge of the measures they can take, they might do nothing to improve security. Therefore, the employees should be educated on which security measures they can take and which risks can be avoided with those measures.

3.1.6 Neutralization theory

Neutralization theory is one of the most known criminal theories, which tries to explain, how criminals justify their behavior. It has been identified in the theory, how individuals justify why they can violate norms, such as laws or polices. (Siponen & Vance, 2010) The theory has been first introduced by criminologists Sykes and Matza in 1957.

Information security policy violations are not criminal acts, as such. However, they violate social norms of the organization and sometimes break the contracts the employee has with the organization. (Siponen & Vance, 2010) For that reason, neutralization theory, as well as the general deterrence theory, have been applied in the IS security studies.

The justifications criminals make are called neutralization techniques, of which Sykes and Matza (1957) introduce five. In addition to these five tech-

niques, other techniques have been identified in the later literature. This study, however, discusses only the techniques found by Sykes and Matza (1957).

- The Denial of Responsibility

The technique of denial of responsibility can be identified in situations where the criminal claims the criminal behavior to be a result of an accident or that the criminal activity was out of his/her control. (Sykes & Matza, 1957)

- The Denial of Injury

The second technique, the denial of injury, can be identified in a situation where a criminal evaluates crime based on whether it has clearly hurt or harmed someone or not. This technique can be identified in a situation where the criminal acknowledges acting against the law, but considers the behavior justified as it has not caused significant harm. (Sykes & Matza, 1957) From the IS perspective, Siponen and Vance (2010) use an example of an employee who thinks it is accepted to violate the ISP's if it does not directly harm the organization.

- The Denial of the Victim

The technique of Denial of the Victim can be identified in a situation, where the criminal justifies the criminal activity by saying the harm caused was deserved or not wrong based on the circumstances of the situation. The criminal usually accepts the responsibility of causing harm or injuring someone but justifies it by saying the target deserved it. (Sykes & Matza, 1957)

- The Condemnation of the Condemners

The fourth technique can be identified in a situation, where the criminal acknowledges the wrong actions, (s)he has made but tries to blame the ones who have been the victims of the crime. (Sykes & Matza, 1957) Siponen and Vance (2010) provide an example of an employee, who violates the ISP and justifies the action by saying that the policy is not sensible, and it is not possible to comply with it.

- The Appeal to Higher Loyalties

The fifth technique can be applied if the criminal defends criminal behavior by acting for the greater good. The criminal may think that to solve a common problem or to achieve a wanted result, law or policies need to be violated. (Sykes & Matza, 1957)

3.2 Organizational level theories

As behavioral theories focus on the employees' personal motivation to ISP compliance, another point of view is to observe the effects of the organizational environment and security climate. Organizational environment and climate, along with top management's attitude towards information security has been shown to affect the employees' behavior and attitude towards information security behavior. This subchapter discusses the previous literature regarding the organizational factors which have shown to influence the behavior of employees.

3.2.1 Factors affecting employee behavior

Banerjee, Cronan and Jones (1998) studied in their research the factors affecting the information security behavior of employees. The study showed that employees' intention to act ethically or unethically was related to their perception of the organizational environment and organization's ethical environment. The study suggests that the more organization is committed to rules and policies, the more likely the employees choose to act ethically as well. (Banerjee, Cronan & Jones, 1998) The organization's attitude towards security has been shown to have effects on the behavior of the employees in other studies, as well. (Kankanhalli et al.; Leach, 2009) These findings emphasize the importance of the organization's and its upper level management's support and example. Based on these findings, the more the organization is committed to their own policies, the more likely the employees are to do so, as well. (Banerjee et al. 1998)

The findings of Banerjee et al. (1998) have been supported also in later studies. As it has been discussed earlier in this paper, information security management requires managerial efforts along with technical solutions. (Luo et al. 2011) Similar finding was made by Kankanhalli et al. (2003) who suggest that top management's support positively affects the employee's intention to take precautions actions. Supportive top management has been shown to be often more willing to allocate their resources towards security acquisitions. (Kankanhalli et al. 2003) It has been shown that the organizational cultures can have either positive or negative effect towards employees' security behavior. When the organization works in line with the security policies, it likely has a positive impact on the employee's behavior, too. (Vroom & von Solms, 2004) This sets up expectations to upper management, which should be leading by example and integrating security in all business operations.

As it was discussed earlier in this study, the research by Leonard et al. (2004) showed that awareness of consequences affects the attitude of an employee to behave in a certain way. This finding is in line with the General Deterrence Theory, which argues that an individual is less likely to engage in criminal activities, if there is a possibility of consequences. Therefore, it is important

for organizations to remind its employees of their ethical policies and the possible consequences of violating those policies.

Kankanhalli et al. (2003) studied the relationships between the organizational factors and security methods. They found in their study that to have effective ISP's, the managers should be actively and visibly participating in the process of creating ISP's. The employees need to be educated on how IS assets are allowed to be used and how they are not. The compliance of ISP's can be monitored by the managers, but it is also suggested to have experienced auditors regularly checking the compliance of the organization's ISP. (Kankanhalli et al. 2003) However, auditing ISP compliance and behavior has been criticized because of its difficulty. Auditing is a suitable method for evaluating the operations of machines or processes, but when it comes to people, their reactions and the factors affecting those reactions vary in different situations. (Vroom & von Solms, 2004) For example password use and the change interval of the passwords can be rather easily monitored, whereas sharing passwords with colleagues is a much more difficult thing to monitor. (Vroom & von Solms, 2004)

Ifinedo (2014) studied employees' IS compliance behavior intentions. He found in his study that if employees were given an environment, where they can, through co-worker socialization, learn about the company values and policies, the ISP compliance was increased. If employees find the compliance to be a social issue, which benefits employees' peers and colleagues, they were more likely to comply with the policies. It was also suggested that compliance can be increased by improving the community spirit. Ifinedo's (2014) findings are in line with the social bond and social learning theory.

Leach (2003) has identified in his research six factors from company culture which affect the security behavior of employees. (Figure 4) The upper section of the figure (parts 1.-3.) consists of the behaviors the employees consider to be the norms and expected behavior of the organization. The lower section (parts 4.-6.) consist of the factors which effect the employees' willingness to comply with the behaviors presented in the upper section.

1. **What employees are told.** This includes the policies and practices which are used for instructing the employees. The requirements for an effective policy are accessibility, coverage, clarity and uniformity. (Leach, 2003)
2. **What employees see in practice around them.** The attitude and behavior of the managers, as well as their consistency with the behavior has been shown to affect employees' attitude towards security. (Leach, 2003)
3. **The user's security common sense and decision-making skills.** Decision-making skills should be encouraged by giving feedback from both correct and incorrect decisions. (Leach, 2003)
4. **The user's personal values and standards of conduct**
5. **Sense of obligation towards employer.** The employees who are satisfied with how they are being treated in their organization usually feel more obliged to their employee and thus feel the pressure to behave as expected. (Leach, 2003)

6. **Experienced degree of difficulty in complying with company procedures.** If organization's policies are easily applicable and they do not add burden to the work of employees, they are more likely complied with. (Leach, 2003)

Also Leach (2003) emphasizes the importance of the managements attitude towards security. Putting an effort in training the employees and showing an example establishes the values of the organization to the employees. The employees' perception of the standard of the expected behavior is formed around the employee and the employee learns the expected behavior from others. When employees can see the way others behave around them, the more likely they will be willing to behave so as well. Therefore, management's efforts can make the whole organization more compliant.

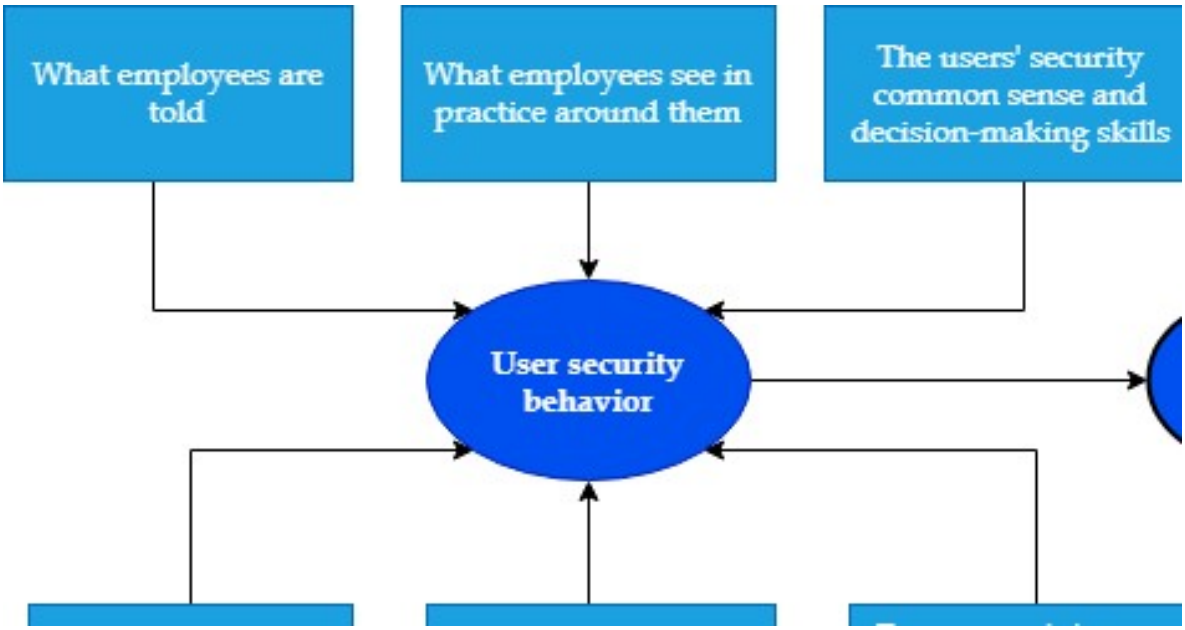

Figure 4 – Factors affecting security behavior. Modified from Leach (2003).

4 SUMMARY OF THE LITERATURE REVIEW

The aim for this literature review was to find out what has been said about employees' security behavior in the previous literature. The literature review showed that the topic has been widely studied. Many factors explaining employees' compliance and non-compliance were identified. As a conclusion of the literature review it can be said that certain behavior cannot be reasoned by one specific factor but rather, behavior is a result of multiple factors. This finding is no surprise, as human behavior could not possibly be explained with one theory or factor only.

The interest in this review is to find out how the employees themselves justify and reason their security behavior and thus the previous literature provides valuable insight of the different viewpoints one can have to observe this phenomenon. In table 1, the different viewpoints found from the previous literature are presented. The table consists of factors, with which the motivation towards compliance can be explained, but also the factors with which the non-compliant behavior can be justified.

The aim of the empirical study is to find out, to what extent employee's security behavior can be explained with these factors. The empirical study aims to answer, which factors employees use to justify their non-compliant security behavior and which motivational factors employees recognize to motivate them to comply with the policies. These questions are answered by comparing the interview questions to the themes found from the previous literature (Table 1) and the results of the empirical study are observed from the viewpoint of these themes.

Factors	Explanation	References
Theory of Planned Behavior/ Intention towards expected behavior	Individuals' personal motivation and intention towards a certain behavior.	Ajzen (1991); Theoharidou et al. (2005); Hazari et al. (2008)
General Dterrence Theory / Risk of punishment or consequences	The higher the risks (e.g. punishments) of a crime (or violation) are, the more likely it is for the person to withdraw from committing the crime.	D'Arcy & Herath (2011); Hu et al. (2011); Theoharidou et al. (2005); Chen, Ramamurthy & Wen (2012); Kankanhalli et al. (2003); Straub & Welke (1998); Guo et al. (2011); Bulgurcu et al. (2010); Leonard et al. (2004)
Social Bond Theory / Social bonds and relationships	SBT suggests that if the individual relies on the strong social bonds, (s)heh as within the individual's group, the less likely the individual is to engage in behavior which is against social norms of the group.	Theoharidou et al. (2005); Hirschi (1969); Ifinedo (2014); Hazari et al. (2008); Chan et al. (2005)
Social Learning Theory / Social learning	Social learning theory suggests that an individual's perception of criminal behavior is formed based on how his/her peers behave and think.	Bandura (1977); Theoharidou et al. (2005); Leach (2003)
Technology Threat Avoidance Theory / Perception of risk	The perception of threat is based on how likely the employee thinks the threat is to occur and how severe the possible consequences of the occurrence of the threat would be.	Liang & Xue (2009)
Neutralization Theory / Justification	A criminal justifies criminal activities or actions which break social norms with justifications, which are called neutralization techniques.	Sykes & Matza (1957); Siponen & Vance (2010)
Company environment	The organization's investments for security and how important the organization considers security to be.	Leach (2003); Banerjee et al. (1998); Vroom & von Solms (2004)
Exemplary behavior of managers	Manager's attitude towards security policies and their consistency of complying with them.	Leach (2003); Pahnila et al. (2007); Luo et al. (2011); Kankanhalli et al. (2003);

		Vroom & von Solms (2004)
Security knowledge	Employees' general knowledge about security and decision-making skills.	Leach (2003); Hazari et al. (2008)
Sense of obligation towards employer	Employees' level of obligation towards employer can affect their will to comply with organization's policies.	Leach (2003)
Quality of company policies	Policies which are easy to understand and apply in everyday routines are more likely complied.	Leach (2003); Pahnila et al. (2007)

TABLE 1. Summary of factors identified in the literature review

5 EMPIRICAL RESEARCH

The goal for this research is to identify, which factors employees themselves consider affecting their security behavior. The research questions examined in this study are:

- *RQ1 What motivates employees to comply with information security policies?*
- *RQ2 How do employees justify their non-compliant ISP behavior?*

Previous chapters strove to examine the research question by reviewing previous literature of the topic. In these following chapters, the research questions are examined by completing an empirical research. This chapter has been organized as follows: chapter 6.1. introduces the goal of the study, the chosen research method and the factors which lead into choosing the chosen method. In chapter 6.2., the way the data was gathered for this study is described. In chapter 6.3., the subject organization of the study is described. In chapter 6.4. the interview process and its contents are discussed. Finally, in chapter 6.5. the analysis method of the data is described and validated.

5.1 Research method

This study has been conducted as a qualitative case study. The data for this study was gathered by conducting semi-structured interviews. Qualitative research method was selected for this study as the interviews enables examining the interviewee's own experiences of the discussed themes. Qualitative study aims to understand and describe a phenomenon, without trying to explicitly measure or generalize it. (Saaranen-Kauppinen & Puusniekka, 2006; Alasuutari, 2012 33-37) As the objective for this study is to understand security behavior of employees, qualitative study was considered as a suitable method for this study.

One of the cornerstones of qualitative study which needs to be taken in consideration is its subjectivity. As the study is conducted in interaction with interviewees, the researchers' objective perceptions are inevitably included. Therefore, one of the important areas of qualitative study is to provide a detailed description of the gathering and analysis process of the research data.

With detailed information, the reliability and credibility of the research results can be assessed. (Sarajärvi & Tuomi, 2017) As the researcher's own interpretation can affect the results of the analysis, it is important to provide enough information of how the conclusions of the study were formed.

One of the research strategies of qualitative research is a case study, which was chosen for this study. Case study is "a research strategy, which focuses on understanding the dynamics present within single settings". (Eisenhardt, 1989, p.534) Case studies aim into either describing a phenomenon, testing a theory or creating a new one. In case studies, one can investigate one or more cases and they can be analyzed by with several different methods. For case studies, the data can be collected from different sources; interviews, questionnaires, archives etc. and the data can be either qualitative or quantitative data, or sometimes even both. (Eisenhardt, 1989) In this study, the data was collected by conducting semi-structured interviews.

This study adopts the single case design. "Thorough examination of a single case study can provide information which exceeds an individual case, although no generalizations can be made based on it." (Saaranen-Kauppinen & Puusniekka, 2006) Based on Eisenhardt (1989), "the goal of theoretical sampling is to choose cases which are likely to replicate or extend the emergent theory." (Eisenhardt, 1989, p.537) This is quite different from statistical sampling, where, through random selection from population, the goal is to show statistical evidence how variables are separated within the selected population. (Eisenhardt, 1989) Although in a case study, random selection of cases is admissible, it is not recommended. (Eisenhardt, 1989) As this study was conducted as a single case study, the interviewed organization was not randomly selected. Also, as the topic of the study is quite sensitive, it was important to consider and select the interviewed organization based on its suitability to this research in order to assure the atmosphere of confidentiality during the interviews.

5.2 Data acquisition

Qualitative interview method is the most common and one of the most important data gathering tools in qualitative research. (Myers & Newman, 2007, p.3) The data for this study was gathered from the information security policy of the researched organization and from interviews conducted with the employees of the organization. The interviews were held as semi-structured interviews. In semi-structured interviews, the interview questions are considered and planned beforehand, but there is room for improvisation and open discussion. Most qualitative research interviews are held using semi-structured interview type. (Myers & Newman, 2007)

Following the method described by Myers and Newman (2007), the outline of the interview was planned beforehand, but the order of the questions and the way of asking the questions alternated between interviewees. However, the themes and content of the interview were the same for each interview. As

the interviews were semi-structured, there was an option to improvise and ask questions which were not included in the preliminary outline of the interview. Being able to rephrase and change the way of asking the questions helped the interview sessions and enabled interviewees to share their experiences better.

Several issues have been identified in qualitative interviews. The artificial situation forces the interviewee to come up with the answers in a short period of time, which can influence the answer negatively. Also, the lack of trust towards the interviewer can result in non-reliable answers. (Myers & Newman, 2007) In this study, the interviewer was familiar with the interviewees, which resulted in open and trustworthy discussions. The interviewees were not given the interview questions in advance, but they were informed of the topic which were to be discussed beforehand. In some qualitative research, the interviews are conducted only on the top-management employees of the organization, which can narrow down the results of the study. (Myers & Newman, 2007) In this study, both managers and subordinates were interviewed. Another issue which had to be considered was the ambiguity of language, (Myers & Newman, 2007) which was solved by defining the used concepts and by asking the interviewees to elaborate their answers in ambiguous situations. The interviewees were also able to ask the researcher to elaborate or readjust the questions.

The interviewees were divided into two groups based on their job description; employees and managerial level employees. Managerial level employees were not necessarily managers, but they were in a position where they were managing one or more subordinates. The interview outlines were slightly different between these two groups, but the discussed themes were the same for both groups. The interview structure was based on the themes brought up in the literature review part of this paper and on the attempt to answer the research question. Based on the themes identified in the literature review, the interview was constructed around these following themes:

1. Perception of social relationships at work
2. Perception of organization's attitude towards security and organization's security environment
3. Interviewee's own perception of security
4. Interviewee's perception of risk
5. Actual security behavior
6. Attitude towards punishment
7. Motivation to comply with security policies
8. Justification for non-compliant security behavior

5.3 Conducting the research

In this chapter, the process of conducting the research is described. Firstly, in chapter 5.3.1, the justification for selecting the case organization is provided. In

chapter 5.3.2 the process of conducting interviews is then described. In chapter 5.3.3 the method for data analysis is described.

5.3.1 Subject of the study

The studied organization requested to stay anonymous, hence the organization or its area of business will not be described profoundly. The subject organization for this study was selected based on its suitability with respect to the research. The company interviewed for this study is a Finnish-based company X. The company operates in Finland in a small industry in the private sector in B2B and is a relatively young organization, which needs to be considered in the results of the study. The organization was familiar to the researcher which helped with conducting the interviews as there was access to the organization's employees.

The organization has approximately 50 employees at the moment. The organization operates in the private sector and their field of operation does not have many external regulations regarding security (except the General Data Protection Regulation "GDPR", which came into effect in Spring 2018). Therefore, the organization was an interesting case to study regarding the subject of the research. Most of the organizations' employees, especially the interviewed employees, have no educational background in information technology nor information security, which also provides a unique viewpoint into regular employees' thoughts towards information security. The organization had no designated person in charge of security, but the interviewees named a couple different colleagues of theirs who had been taking care of some sectors regarding security, such as GDPR. Some of interviewees considered that the responsibility of security and monitoring compliance should not be a responsibility of only one person.

> "It shouldn't be on the shoulders of one person, who's not with every employee every day. Rather, it should be implemented to those who are in managerial position, in other words, to every manager."

In addition to the familiarity and the suitable size, the young age of the organization made it an interesting case to observe. The organization has grown significantly in the past years, which has forced the organization to change its ways of working, including security. Transforming from a small startup to a big organization does not come without challenges and it was an interesting time to observe the thoughts of the employees.

The organization has an information security policy, which, directly translated, is named "privacy protection policy". The policy includes specific instructions for security requirements, as well as an explanation for privacy protection and its goals. The policy also includes instructions for possible data breach situations. The policy had several instructions, but for this study, we chose four instructions which were investigated more thoroughly in the interviews. The instructions were chosen based on which instructions were the most relevant

for the job descriptions of the interviewed employees. The chosen instructions were the following:

- Change your passwords regularly
- Lock your work computer and/or mobile phone when left unattended
- Use protective shields in your work computer when working on a public place or public transportation
- Never share your passwords or other user identification with anyone, including colleagues

All the employees of the organization were allowed to work from home, and for some of the employees, the job requires remote working from time to time. Most of the interviewees estimated that they usually work from home at least once a week. The length of the employees' employment varied from a couple of months to 2-3 years.

5.3.2 Conducting the interviews

The interviews were conducted in April 2019 during two separate days. 9 employees of the studied organization were interviewed. The organization was allowed to choose the interviewees themselves, but it was requested that the employees would be working in different areas of the business. The interviewees' job descriptions varied broadly from each other, but to ensure the anonymity of the organization and its employees, their job descriptions will not be further described. All the interviewees had been working on the organization for at least half a year, so they had good understanding of the working methods of the organization.

The interviewees were in either employee or managerial position. The managers were in a position where they had one or more subordinates. Three out of nine interviewees were in a managerial position, six were in an employee position. The interviews were conducted individually. The interviews were held in the organization's office space, in separate meeting rooms. All interviewees gave their consent to record the interview. One interview was made through a phone call, but the rest of the interviews were conducted face-to-face. The phone call couldn't be recorded, but precise notes were taken from that interview.

The length of the interviews varied from thirty minutes to sixty minutes. The recordings of the interviews were transcribed as soon as possible after the interviews, so that the contents of the interviews were better recalled by the interviewer. As all the interviewees were native in Finnish, the interviews were conducted completely in Finnish. The analysis of the contents of the interviews was conducted from the Finnish transcripts, but the quotes used in this paper were translated into English to the best of the researcher's ability. Colloquial

phrases were not translated but the message of the interviewee was preserved as well as possible.

As most of the interviewees had no previous experience with information security, the researched topic was first defined. The interviewees were asked to describe their perception about which they considered to be the most important assets of the organization, which the information security policies aim to protect. An interesting observation from the discussion was the difference between each answer to this question, as all the interviewees answered differently. Interviewees considered assets such as customer data, contract information, their products and trade secrets to be the most important assets. The dispersion of the results shows the importance of defining what information security aims to protect.

5.3.3 Data analysis

As the interest of this study is in the way the interviewees argue, characterize and justify their thoughts and behavior, the approach for this analysis can be considered relativistic. (Saaranen-Kauppinen & Puusniekka, 2006) Relativistic analysis focuses on the way individuals describe their own perceptions and how they justify their behavior. Another form of analysis is realistic analysis, which focuses on the phenomena itself, and less on how the phenomena is described or discussed about. Relativistic analysis is focused on how individuals justify and describe their viewpoints and perceptions. (Saaranen-Kauppinen & Puusniekka, 2006) Although the actual behavior of employees will be discussed in the results, their compliance or non-compliance is not the focus of the study, but rather the way they justify and explain either behavior.

After the interviews were conducted, the interview records were transcribed. As the used language itself is not the subject of the study, no special characters were used for the transcriptions of the interviews, but all the interviews were transcribed word-to-word. After the interview recordings were transcribed, the transcriptions were coded with colors based on the similar topics and themes discussed in the interviews. Coding helps the researcher to piece together, which parts of the research data are about the same topic. (Saaranen-Kauppinen & Puusniekka, 2006) Coding means that the phrases, sentences or paragraphs of the text are labeled or categorized to organize the information of the study. (Basit, 2003) In practice, the coded sections of the document were highlighted by the researcher's selected colors.

The data gathered from the interviews was analyzed by using a thematic content analysis method. Thematic content analysis was method was chosen for this study, as it is especially suitable for analyzing semi-structured interviews. The method requires that the interviews are fully transcribed (Burnard, 1991), which has been successfully carried out in this study. The aim for thematic content analysis is to "produce a detailed and systematic recording of the themes and issues addressed in the interviews and to link the themes and interviews

together under a reasonably exhaustive category system". (Burnard, 1991, p.462)

Thematic analysis can be conducted based on the data or based on existing theories or frameworks. Data-based analysis aims in finding connecting factors from the text, theory-based analysis forms themes based on existing theories. Thematic analysis is especially suitable for analyzing data from interviews, where the interview structure has been built on themes. The themes found from the data imitate the interview structure very closely. The selected parts from the interviews, which were previously coded, are then arranged under identified themes. (Saaranen-Kauppinen & Puusniekka, 2006) This research was conducted as a thematic analysis and was based on existing theories and literature.

5.4 Theoretical framework

To examine the results of the study, the framework used to observe this phenomenon should be described. In the literature review, the multiple theories explaining individuals' security behavior were discussed. Although it would be beneficial to combine a framework from each of the theories, it would expand the research unnecessarily extensive. However, the results of the interviews were reflected on the findings of the literature review. The interview data was grouped based on

The findings of the literature review included the following factors:

- Intention towards expected behavior
- Risk of punishment or consequences
- Social bonds and relationships
- Social learning
- Perception of risk
- Justification
- Company environment
- Exemplary behavior of managers
- Security knowledge
- Sense of obligation towards employer
- Quality of company policies
- Personal values

5.4.1 GDPR

One of the topics which came up in all of the interviews, was the General Data Protection Regulation, "GDPR". The regulation came into effect on May 18th, 2018, almost a year before the interviews for this study were conducted. The

regulation applies to every organization, who handle and process personal data, such as customer or user information. GDPR sets legislative requirements regarding data subject rights, including handling, storing and removing personal data. Breaching or acting against GDPR is punishable by penalties. (EU GDPR.org, 2019)

GDPR received lots of media coverage before and after it came into effect, thus affecting the operations of every organization handling any customer and/or user information. In the interviews conducted for these studies, many of the interviewees interlaced information security with data protection, to both of which the organization had policies for. As GDPR was discussed in every interview and it is discussed in the results of the study, it was a necessary concept to provide a definition for in this paper as well.

6 THE RESULTS

In this chapter, the results of the empirical study are presented. The case study aimed in finding answers for the two research questions regarding employees' information security behavior. This chapter has been organized around three main themes. In chapter 6.1 the employees' perception of their own ISP compliance is compared to their described actual behavior. In chapter 6.2. the reasons employees gave for complying with security requirements are presented. In chapter 6.3 the strategies employees used to justify violating the security policies are discussed.

6.1 ISP compliance perception vs. actual behavior

In this subchapter, the interviewees' perception of their ISP compliance and their actual security behavior are compared.

6.1.1 Background of the interviewees

For this study, 9 employees of the organization were interviewed. There were total of three male interviewees and six female interviewees. None of the interviewees were professionals in information security. The interviewees were grouped in two categories based on their job description. The interviewees were either in an employee position where they had no subordinates or in managerial position where they had one or more subordinates. As the organization is very small, further background information is not specified to assure the anonymity of the interviewees. As security behavior is a sensitive topic it was important to make sure the interviewees can't recognize each other from the results.

The interviewees' names were replaced with "Interviewee" and they were individualized with numbers from 1 to 9. In table 2, the interviewees' positions are classified. As the organization has been operating for only a couple of years,

none of the employees had been working in the organization for a long time. The newest employee interviewed had been working in the organization for four months. However, all the interviewees were familiar with the organization's procedures and operations.

Interviewee	Position (Manager position / Employee
Interviewee 1	Manager position
Interviewee 2	Manager position
Interviewee 3	Manager position
Interviewee 4	Employee
Interviewee 5	Employee
Interviewee 6	Employee
Interviewee 7	Employee
Interviewee 8	Employee
Interviewee 9	Employee

TABLE 2. Information of interviewees

6.1.2 Actual security behavior

To examine the actual security behavior of the interviewees, the interviewees ere asked questions related to their usual behavior. The questions were based on the instructions specified in the organization's ISP. In table 3, the results of the discussions are presented. The abbreviations of the questions are presented in the table, the complete questions asked were as follows:

1. Have you read your organization's Information Security Policy?
2. Do you consider yourself to be complying with the policy?
3. Do you think it would be likely for your organization to face security threats or security attacks?
4. Do you have a privacy shield in use?
5. Do you lock your computer every time you leave your computer unattended?
6. How often do you change your passwords?
7. Have you ever shared your password or been given someone else's password?

	I1	I2	I3	I4	I5	I6	I7	I8	I9
Has read ISP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Complies with ISP	Yes	Yes	Yes	Yes	Yes /No	Yes	Yes	N/A	Yes
Security threat likely?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Privacy shield	Yes	No	No	Yes	No	Yes	Yes	No	No
Locks the computer	Yes, always	Yes, usually	Yes, usually	No	Yes, usually	Yes, always	Yes, usually	Yes, always	No
Password change	Never	Never	Never	Some-times	Never	Never	Never	Never	Never
Shared password	No	Yes	Yes	No	Yes	No	Yes	No	Yes

TABLE 3. Summary of interviewees' described behavior

This table shows a major collision between the employees' perception of their security behavior and their actual security behavior. One of the possible explanations for this finding is that for some employees, there had been a long time in between the last time they had read the policy. Therefore, it is possible that they did not recall the contents of the policy. However, all interviewees except one and the interviewee who had not read the policy, were sure they were complying with it. These results can show that either the interviewees really did not recall the contents of the policy or they genuinely believed their security behavior is compliant and they behave correctly even though that is clearly not the case.

If the results are examined more closely, seven interviewees answered they considered themselves to be complying with the security policies and one interviewee said that (s)he probably does not comply with them daily. One of the interviewees had not read the policy but considered himself/herself to behave compliantly. Those interviewees who said they were complying with the policies, also all admitted that there were things they could be doing better. Interviewee 3 notes:

> "Yes, I do (comply with the policies), at least I do pay more attention to these things these days, but I'm sure that there is even more I could do." (Interviewee 3)

Interviewee 7 admitted having change resistance in the beginning because (s)he did not consider the security practices to be necessary. Despite having prejudice, the interviewee said that nowadays (s)he tries to be compliant.

> "I try to, let's put it that way. At first, my thought was that do we really need to be locking our computers in a closed office, since we all have the passwords for the same systems, so why do I need to lock my computer when I leave the office. But it's the little things that I've improved since the reform (GDPR) came." (Interviewee 7)

Again, this point of view emphasizes the importance of educating the employees about the reasons for applying security policies; why these actions are necessary and what are the possible risks if policies are neglected. As the comment from this interviewee shows, not understanding the reasons behind the policies can create resistance towards them.

Another question regarding security behavior was about the use of privacy shields. Simultaneously to launching the ISP, the employees had been asked to fill out a questionnaire of whether they wanted to have the protective shield ordered or not. Three out of nine interviewees said they had the protective shield and they were using it when working outside the office and sometimes also at the office. Four out of nine interviewees said they did not have the protective shield, but they did not need it. One of those interviewees said to be working regularly remotely and in public places, as well. Two out of nine interviewees said they did not have it but considered that they should have it. Interviewee 2 summarizes:

> "No, I don't have it. – We had an inquiry on who's ordering it, and I answered that I'd like to have it. I never got it and I haven't been asking for it. "(Interviewee 2)

Interviewee 3 recalled similarly, as they had ordered the privacy filters but never received them. Neither of the interviewees had no certain information of the reasons behind the withdrawal of the order.

> "At one point it was discussed that we would get privacy filters for our computers, but I think we never got them. I, myself, ordered them a long time ago but we didn't get them, because apparently, they were somewhat expensive or something. At least my team did not receive them, and apparently other teams didn't either." (Interviewee 3)

Some of the employees had been informed that the privacy shields were ordered only to those employees who regularly work remotely or who handle sensitive data (e.g. employee's identity numbers or salary information etc.). However, some the interviewees had not been informed that the shields would not be ordered for everyone. Informing the employees would have cleared the situation. Informing the employees would also have been beneficial as the organization could have stated, which situations require privacy shields to be used. In this way, the employees could ask for the shield if their work habits changed in a way which required the shield to be used.

> "No. (I don't have it) As far as I've understood, we've taken a controlled risk, as they are such a big investment, so they have been given to those who are in a situation where there might be at risk." (Interviewee 9)

Secondly, the interviewees were asked if they would always lock their computers when leaving the computer unattended. Six out of nine interviewees said that their computers locked automatically after 5-10 minutes. Of those interviewees, most of them said that they do not usually remember to lock their computers, but they knew that they would automatically lock after a while. Three out of nine interviewees said that they would always lock their computers when leaving them unattended.

The interviewees were also asked, had they noticed if their co-workers were always locking their computers when they left them unattended. Interviewee 3 notes:

> " No, I don't think so. At least what I've noticed. – probably similarly to what I do, people sometimes leave them just open, or turn the computer screen a bit closer, but I don't think that very many would actually lock the computer fully. I think most have set it to lock down automatically in a few minutes or so." (Interviewee 3)

Quite interestingly, it appeared that many of the interviewees, as well as their co-workers had a habit of leaving their computers unlocked, knowing that the computer will lock itself automatically in ten minutes. Although automatic locking is more secure than not locking the computer at all, the habit of leaving their computers open leaves the option for insiders with malicious intentions. Knowing the delay for locking gives insiders with malicious intentions a perfect slot to carry out possible attacks.

Thirdly, regarding the password sharing, it turned out to be a difficult question to answer. Four out of nine interviewees remembered a situation or multiple situations where they had shared their passwords or someone else had shared their passwords with them. Four out of nine interviewees said they had never shared or been shared passwords. One interviewee was not sure and did not recall such a situation. Interviewee 9 notes:

> "I do kind of remember one situation where I had to give my password to my colleague, but it was not to one of the most critical systems we have." (Interviewee 9)

Although the interviewee did not consider the system the passwords was given to be their most critical one, the issue of sharing the password is in the possibility of having the same password in other systems as well. It might also reveal the password logic of the employee, if his/her passwords all follow the same pattern and might expose the employee to risks if the passwords are never changed. The fourth question is highly linked to this issue, as the interviewees were asked about their routine of changing their passwords.

It was discussed how often interviewees changed their passwords and if they had any kind of a routine for changing the passwords. Surprisingly, nine out of nine interviewees said that they did not regularly change their passwords. This information conflicts with the interviewee's thought about complying with the security policies, as seven out of nine interviewees considered themselves to be compliant. This factor can have a simple explanation, if the

interviewees did not remember that such a policy existed. Interviewee 3 admitted having the original passwords in use, meaning the passwords had never been changed.

> "Very rarely. Too rarely. They probably should be changed, I think I still have the original ones in every system." (Interviewee 3)

Interviewee 6 recalled changing the passwords once during his/her time in the organization.

> "I don't (have a routine). I haven't changed the passwords probably for once after I've started working here." (Interviewee 6)

Interviewee 2 noted that since they have to use so many different systems daily, it would not be realistic to remember and change passwords for each system. The interviewee also had the same password in some of the systems. This exposes several user accounts to threats if the same passwords are used in every system and especially if they are never changed.

> "Extremely badly. Especially when you start to have passwords for everything, you should remember something like 20 passwords and they also are the same ones for each system, so I don't even have separate passwords for different systems. – I very rarely change them, if at all." (Interviewee 2)

> "No, I don't change them." (Interviewee 5)

Never changing the default passwords makes the user account more vulnerable even if the default password was complex and lengthy enough. n interesting Observation regarding the previous chapter, where the employees' perception of risk was discussed, was that those employees, who didn't consider the risk for a security threat or violation to be likely, were complying less with the policies. Therefore, it could be easy to come in to a conclusion that perceived risk influences the security compliance. The employee's perception of risk is discussed further in the next chapter.

6.1.3 Perception of risk

In this part, the interviewees' perceived risk of security threat is discussed. Based on technology threat avoidance theory 'TTAT', an employee takes protective measures based on how likely and severe the employee perceives the threat to be. In other words, the less likely the employee considers the threat to be, the less likely the employee is to take safeguarding measures. (Liang & Xue, 2009) The interviewees were asked how likely they considered it would be for the organization to face security threats or security attacks. Seven out of nine interviewees found the risk for a security threat or security attack towards their or-

ganization to be likely or very likely. Interviewee 3 summarizes, that since anything seems possible, security threat would not be surprising either.

> "I wouldn't be surprised if someone tried to access our information, somehow I'm taking nothing as a surprise nowadays." (Interviewee 3)

Interviewee 1 considered the publicity of the organization and the fact that it might be of interest for some parties to attack them. Publicity can result in different feelings towards the company and especially negative feelings can create a motive for a security attack.

> "I think it would be quite likely at the moment. We are quite a visible organization, and I think we resonate both positive and negative feelings in most people, so I find it quite likely." (Interviewee 1)

Interviewee 8 noted that the organization handles a lot of important information, which might interest some parties, but thought that mainly the security threat would be about causing disadvantage to the organization. The interviewee did not consider the organization to possess anything important enough for someone to attack them to get access to that.

> "Well yeah it is likely. I would imagine it would be more about wanting to cause mischief than, yeah. If you think about it, we handle a lot of important information, so why not." (Interviewee 8)

However, some of the interviewees considered the risk for a security threat to be non-likely. Interviewee 9 noted that since they rarely have visitors coming into their office, and it is even more rare for a visitor to come to the office without an escort, the risk of security threat is very low.

> "In our office environment we, in principle, have only our own employees, so as such, there is no need to worry." (Interviewee 9)

However, this line of thought does not take into consideration the possibility of insider threat. Therefore, the organization cannot content itself to protecting its information from outsiders, but insiders should be considered as well. Interviewee 9 also considered the risk to be unlikely, because the organization would not be an interesting target enough for someone to take the trouble. One of the introductive questions asked in the beginning of the interview was about the IS assets of the organization and what the interviewee considered them to be. From this comment, it can be observed that it would be important for the organization to make clear which the important assets are and why they need to be secured. Every organization holds assets, such as information and data they want to keep secure and the assets should be known by the employees as well.

> "It's unlikely. The risk for someone to be that interested in our things to make an effort to access our information… I think that it's not seen as such a big risk, which is why we're not overly cautious about it." (Interviewee 9)

Interviewee 7 pointed out that (s)he is unfamiliar with the topics related to security, so (s)he found it hard to evaluate the likeliness of such threat. Another important topic of education for the organization would be the possible threats the organization might face. Interviewee 7 notes:

> "Well I wouldn't find it (the risk) to be very likely. We have all the systems and such, so if someone outsider tried to access them, they shouldn't be very easily accessed." (Interviewee 7)

The importance of educating employees about the possible risks of non-compliance and the possible threats there might be to the organization is clear. Unauthorized access can be given to an intruder in many ways and the employees should acknowledge where the risks lie. It might be useful to educate the employees about information security, and the reasons for the policies they have in place and what can result from non-compliant behavior.

Quite interestingly, the results show that despite how likely the interviewees considered the risk to be, the risk was, in every interview, considered to be coming from an external source. This line of thought probably affected especially the answers of the interviewees who did not consider the risk to be likely, as they thought their information to be safe as outsiders would not be able to access them either digitally or physically. The interviewees who considered the risk for a threat to be likely, most often justified the thought by the visibility and the publicity of the company. The culture of trust surely creates an environment where it is assumed that no employee has malicious intentions, but it should also be considered. It could be argued that strong social bonds can encourage the employee to act compliantly but it might blind the employees from a possible threat coming from the inside of the organization.

As the interviewees' own perception of security threat affects their attitudes towards security, it was also important to discuss how the employees view the security environment of the organization and if they considered information security to be something the organization was investing in. All the interviewees thought that although these topics have been discussed, it is something that could be addressed even more. Interviewee 8 summarizes the issue by saying that information security should be reminded more frequently and there should be collective rules for everyone. This thought could be interpreted in a way that ISP's are not considered as rules, or that only some of the employees consider them to be. Interviewee 2 points out that ISP compliance is somewhat related to every employee's own individual customs and routines. Therefore, the efforts of the organization would be much needed to set the standards for security behavior.

> "I'm sure that in a theoretical level, yes. In practical level, there is always something to improve. It has been well invested in a way that things are really discussed together, and it is required that every employee reads through certain things and follows certain standards. But it is very much related with individual customs on how everyone understands certain things, so I think it could be focused on even more." (Interviewee 2)

Interviewee 9 highlights that although they could have been instructed more, the organization trusts their employees in a way that everyone is considerate about their behavior and thus acknowledges their actions.

> " I don't know how, for example, new employees get the instructions and how well they are taught, I myself have felt that I've been well instructed. Although I have also felt that we could have been instructed more strictly and more could have been expected from us. In our company, everyone's own responsibility and thinking is emphasized, so that everyone knows what they are doing." (Interviewee 9)

Interviewee 7 considered the organization has already taken steps to the right direction, especially after the introduction of GDPR. Interviewee 7 also states that the organization should make sure that all the employees are educationally in the same level regarding security, despite how long the employee has been working on the organization.

> "I think now that the GDPR came into effect and our company is growing and we have new people coming into our office, it would be important that we would be on the same page about what our policies and practices are. Although I think that after the reform (GDPR) we have invested in it more." (Interviewee 7)

Previous study by Banerjee, Cronan and Jones's (1998) showed that employees' intention to comply with policies was related to their perception of the organization's level of commitment towards rules and policies, as well as the general ethical atmosphere of the organization. Thus, it was asked from the interviewees, how information security showed in their organization and if it was something the organization was investing in.

In the first half of the interviews, the interviewees were asked to describe, which assets they considered to be the most important assets for the organization to protect. It was then asked what kind of measures were taken to protect those assets.

> "We have the kind of systems which require passwords and we are sometimes reminded that passwords need to be changed and so on. Then we also have instructions on how to act and in that way everyone, in principle, knows, or at least I hope everyone knows how to operate." (Interviewee 9)

One of the interesting points brought up in the interviews was the managements' trust towards the employees. As interviewees 4 and 9 emphasize, the organization has the kind of culture where everyone carries the responsibility of their own actions. This kind of culture encourages and trusts the employees to use common sense and act in the best interest of the company. It can be concluded that the organization has, at some point, invested in information security more but in the course of time, the level of investment has decreased. As interviewee 9 noted, the organization's culture is largely built on trust towards employees, which can lead into a thought that ISP does not need to be reminded of.

A thought which was brought up in many of the interviews was about regular education. The interviewees felt that security should be reminded more often, and the organization should make sure all the employees are on the same page about the organization's policies regarding security. The interviewees were asked if their organization had arranged or if they had participated in any kind of security training after their orientation in the beginning of their employment relationship.

> "Well, we haven't had very many of them. I think we had one session where we went through it more thoroughly. We haven't had that many training sessions or anything like that. I think it would not be harmful if we had training sessions at regular intervals, because our employees change a lot, even though new employees had discussed it during their orientation. Then the old and new employees would be on the same page." (Interviewee 3)

> "I don't remember being in any kind of training. Maybe we had a remote meeting or something for all our employees, where we were instructed, and things were talked through very generally. Besides that, there hasn't been any (trainings). (Interviewee 7)

Interviewee 4 considered the organization to take care of information security as is required, and everyone has a positive attitude towards security policies. Aligned with Interviewee 9, this thought underlines the importance of the employer's trust towards employees.

6.1.4 Summary

To summarize this chapter of employees' perceptions about compliance and their actual security behavior, it can be argued that there were significant differences between employees' perception of their behavior and their actual security behavior. Two of the most neglected ISP instructions were changing passwords and sharing passwords with colleagues.

Another theme discussed in this chapter was the interviewee's perception of security risk. Two out of nine interviewees considered there is no threat of security risk for the organization. Seven out of nine interviewees considered that there is a risk of a security threat. Two of the interviewees who considered there to be no risk also did not recall complying with the security policies discussed. However, similar results were observed from the interviewees who did consider there to be a risk of security threat. Therefore, no conclusions can be made of the connection with perceived risk and actual security behavior. It would, however, be beneficial for the organization to educate its employees about the possible threats. When introducing new policies, the organization should emphasize why such policies are put to use and from which threats instructions are protecting the organization from.

6.2 Motivation for compliance

In this subchapter, the first research question, "*What motivates employees to comply with information security policies?*" is examined. The research will go through the motivational factors which were identified from the interviews and they are mirrored to the factors found in the literature review. The interviewees were asked what motivates them to comply with the ISP and in this chapter, the findings of these discussions are discussed.

6.2.1 Social bonds and social learning

In this part of the study, the social bonds and relationships of the employees are discussed. Social learning is also covered, as it is highly affected by the level social bonds. The interviewees were asked to describe their relationship with their co-workers and how close they felt their co-workers were. Although the question itself does not prove the social bond theory, it gives an overview to the relationships and the atmosphere of the organization. Al interviewees considered themselves to be friendly with their co-workers, and most of the interviewees had co-workers who they were closer with also outside work. Most of the interviewees said that they were comfortable to share also non-work-related things with their co-workers. Interviewee 9 emphasized that the reason (s)he likes to work in the case organization is because of the relationships and the leadership of the organization:

> "The colleagues are the most important reason why I like it here. It's the kind of spirit and how things are led and how things are done here." (Interviewee 9)

Interviewee 2 addressed the open culture of communication in the organization and their ability to discuss any subjects freely.

> "Yeah, they (colleagues) are close to me in a sense that we share also other than work-related things with each other. Our culture of communication is very open, and we can speak frankly, which is kind of the reason why I like it here and why probably everyone likes it here, as well." (Interviewee 2)

Relationships between colleagues was an important topic to address as the social bonds' employees have can influence their behavior. All the employees considered at least some of their co-workers to be rather close, although Interviewee 6 pointed out that his/her relationship is a bit different with his/her boss than co-workers.

> "With my co-workers, yeah, I'm relatively close, so that I know what they are doing in their free time. With my boss, I am not as close as I am with my co-workers, but (s)he is also the kind of a person with whom I can discuss if I have any serious stress in my life." (Interviewee 6)

Two of the interviewees felt that in a constantly growing organization which has employees in several offices, it is not realistic to be close with everyone. However, they felt that they were close with the people they had been working the longest and most closely with. Interviewee 1 notes:

> "It depends on the co-worker. I'm very close with some of them and very distant with some of them. -– Now that we have a lot of people working here and the people chance a lot, or, should I say, regularly, it is not possible to become friends with everyone." (Interviewee 1)

All the interviewees considered themselves to be close with at least some of their co-workers. Discussing the social relationships and bonds was necessary from the viewpoint of social bond theory, which claims that strong social bonds can prevent an individual from committing a crime. (Theoharidou et al. 2005) The level of compliance towards social norms is said to be heavily dependent on the attachment on other people. An individual's willingness to gain or maintain social status is also shown to lessen the likeliness to commit a crime. (Theoharidou et al. 2005) As social bonds and feeling of belonging has such a big effect on the behavior of individuals regarding criminal activities, it was an important topic to discuss in this study as well.

Hirschi (1969) had identified different types of social bonds. One of them was commitment, which meant that if an individual is trying to gain or maintain social reputation, the individual usually tries to avoid engaging in criminal activities as it might negatively affect their status. When asking about the motivation to comply with policies, Interviewee 7 answered that s(he) would not want to be the one causing trouble for the organization. This can be interpreted as wanting to maintain status in the work community and causing trouble for the organization might affect that status.

> "Maybe it's just that you don't want to be the person causing something or that you would have to say that something happened because of your own carelessness." (Interviewee 7)

Associated with social bonds, social learning also needs to be addressed. As it has been discussed earlier in this paper, the social bonds, learning from peers and even social pressure can affect the behavior of employees. Social learning theory aims to explain how the things around an individual affect the individual's intention to engage in criminal behavior. (Bandura, 1977; Theoharidou et al. 2005) Although security violation is not criminal behavior as such, the theory can be applied in the context of security violations. The theory of social learning is supported by Leach (2003) who found that one of the factors affecting employee security behaviors is the example they receive from their colleagues and managers. During the interviews, interviewees were asked about their behavior related to complying with their ISP's. During the conversation regarding the instruction concerning unattended devices the interviewees were asked if they had noticed if their colleagues followed that instruction. Interviewee 9 summarizes:

> ” Well, I think that it is something that we’re a little careless about. In public places everyone takes care of things very well, but in our office, where our doors are open, and we sometimes have customers visiting, people tend to be a little careless with locking their computers. But it is so rare that we have visitors here, much less that they would go to our rooms, so I think the experienced risk is quite low. I think that’s the reason why people are not so careful with that.” (Interviewee 9)

It can be interpreted that the employees allow non-secure behavior in their office but are cautious outside the office. Although it is positive finding that the employees are cautious outside the office, the same should apply inside the office, as well. Although social learning from peers can encourage an individual to behave in an expected way, it can also backfire in a situation where non-compliant behavior is encouraged by peers. It could be argued that strong social bonds can create positive results through social learning, but the example and atmosphere provided by peers should encourage to be compliant and not to allow slipping from the policies.

6.2.2 Risk of punishment as a motivator

The General Deterrence Theory is one of the most used theories for explaining information security behavior (D’Arcy & Herath, 2011). The Deterrence Theory claims argues that an individual evaluates, whether or not to engage in criminal behavior based on how likely and severe the possible sanctions are, as well as how big the reward for that behavior is. (D’Arcy & Herath, 2011)

To get an understanding of the organization’s current situation regarding monitoring and punishing non-compliant behavior, the interviewees were asked if their security behavior was monitored and how it showed in their daily basis. Some of the employees said that they had been reminded of the policies by their supervisors. It was also discussed that employees sometimes reminded each other of the policies, for example if they noticed someone leaving their computer open. Interviewee 3 considered monitoring employees unnecessary, as the organization can trust their employees to behave as expected if they are reminded of the policies regularly.

> “Yes, if someone like, notices that you’re doing, like if you do something against the instructions or forget to do something you should have done, I’m sure that someone is keeping an eye on those things, but not on our every move.” (Interviewee 7)

> ” In practice, it (compliance) is not monitored. In obvious situations, like if you see that someone has left his/her laptop unlocked in the table and you can clearly see that it is not locked, then it is pointed out but otherwise, no.” (Interviewee 1)

Based on General Deterrence Theory, the individual might not commit a crime if the risk of sanctions was high or the sanctions were severe. As the theory suggests that the possibility of a sanction would restrain individuals, or employees, from engaging in criminal or non-compliant behavior, the employees

were asked how they would react if their organization started giving sanctions or punishments for non-compliant behavior. Interviewee 5 considered punishment to be something that would make you upset and would prefer positive manner of approach.

> "Yeah well, I would prefer the carrot over the stick. Rather by fair means than foul. If you get punished in any area of you work, it starts to piss you off." (Interviewee 5)

Interviewee 9 also considered punishment to be a negative manner of approach and would prefer constructive discussions rather than getting punished for unwanted behavior.

> " The kind of culture of leadership, where things are solved with punishments or warnings, is something I don't think highly of. I could find it as an unfortunate way to approach these things. More than that, I would hope that if these things are noticed, they would be mentioned and brought up, and they would be taken care of that way. – As long as people behave, in principle, sensibly and carefully, it would feel unreasonable to punish with a sanction as the situation could be handled by instructing the person to not do it again." (Interviewee 9)

Some of the interviewees did not consider the idea of punishment to be completely ruled out. Those interviewees who considered punishment to be something worth considering, thought that it would help themselves to comply with the policies more efficiently.

> "I don't know, punishments and sanctions are always primarily an unpleasant thing. On the other hand, you would probably start to pay attention to it more, so it could have that kind of a consequence. I think it wouldn't affect my working that much other than I would change my passwords more often – I don't see it as a good solution, but I won't say that it wouldn't be an effective solution." (Interviewee 8)

One of the interviewed managers considered the effect an implementation of punishment would have on the general atmosphere of the organization. It was pointed out that employees are bounded by contracts, which bound the employees to act on the best interest of the organization and by the company's policies. The ultimate punishment for breaking the contract would be annulling the job contract, but the interviewee does not consider other types of punishment applicable in this organization.

> " I wouldn't apply it to our culture, I just thought about it, how hard it would be to push through a model of sanctions for non-compliance. -- I would consider a more humoristic approach, as it is, after all, an important issue. Or, rather, we should reward those who have complied with the policies extremely well rather than by giving sanctions. – Surely, if we think about an extreme situation, we have certain terms all our employees sign. – In an extreme situation, that is the sanction that we act based on terms of employment and the job contract is annulled. But otherwise, no." (Interviewee 1)

6.2.3 Obligation towards employer

One of the motivational factors identified in the literature review was obligation towards employer. Many of the interviewees felt obliged to the organization and considered the interest of the company to be one of their motivational factors. Interviewee 2 notes:

> "…nowadays anything can result in a lawsuit, especially if we're talking about these issues (security). Especially the emails you send to external recipients, you acknowledge that it could end in a big stir and the whole organization would naturally be a part of it. That's the reason why you pay more attention to our daily, internal operations." (Interviewee 2)

Especially after the GDPR, the possibility of a lawsuit has become more concrete to many of the interviewees. The loyalty towards the employer motivates Interviewee 2 to comply with the policies. The viewpoint of legal consequences was brought up by Interviewee 5, as well. His/her viewpoint differed from Interviewee 2's viewpoint, as Interviewee 5 consider the personal accountability the employees have if they break their contracts. Therefore, breaking the company values and policies would not be beneficial which motivates the interviewee.

> "...maybe avoiding a catastrophe. I don't think it would pay off, if someone from the organization behaved unethically on purpose. We signed some contracts, didn't we, or at least we have verbally agreed that we don't act against the values of the organization. I think it could lead into a lawsuit or something." (Interviewee 5)

Interviewee 1 was answered that maintaining the image of the organization and thus the business has been the biggest motivator. Negative publicity can rise from data leaks which can have a big impact on the business of an organization.

> "Well, the business and maintaining the image of the organization is the biggest motivation for me." (Interviewee 1)

The connection between the employee behavior and the General Deterrence Theory could be observed from the perspective of external factors, such as legislation. As it was discussed earlier in this paper, GDPR came up in all of the discussions during the interviews. To investigate the interviewee's possibly differing views towards punishment coming from an external or an internal actor, the interviewees were asked about their views towards the regulations of GDPR and if they found their compliance towards those regulations to differ from the compliance towards their organization's policies. Interviewee (x) noted:

> "Maybe along with the GDPR I've become more precise and aware about all those things, as there can be such harsh penalties. So, you need to comply with them and that way you have become more precise with it and you always remember to remind the customers about it, as well." (Interviewee 8)

From this quote, the fear of sanctions can be identified. Although GDPR penalties are not given to individuals, the threat of causing penalties to the organization motivates the employee to comply with the policies. It could be argued that the external factors do influence the compliance of the employees.

> "Well, complying with GDPR motivates me because we want to protect the individuals who participate in our operations. We do business with trust. So, it is unambiguously so that we need to be trusted and that's why I comply with it (GDPR)." (Interviewee 5)

Interviewee 5 brought up an interesting point about the importance of complying with GDPR. In this case, it can be argued that requirements coming from an external source motivate the employees to be more compliant, since the interviewee found that GDPR should be strictly complied. However, the employees are not seeing the link between their own security policy compliance (such as password change) and GDPR requirements. Although changing passwords regularly is not required in the GDPR, it is a practice which assists the security of user information. An important topic to be discussed with the employees would be that to what extend the compliance of security policies affect the whole organization and the customers of the organization, as well.

Another topic discussed with the interviewees was their motive to comply with the organization's policies. Many of the interviewees said that the biggest motivator for them was the unwillingness to cause trouble or loss of reputation for the company.

> "It's probably just that I don't want to cause this company a loss of reputation or any kind of damage, so maybe that's the biggest motivator for me. – So maybe the company reputation and that I don't want to be the one causing some kind of chaos here. And, in some cases the people whose information we handle need to be considered so that we wouldn't cause trouble to them. If it would happen that the information was leaked somewhere, I would hope that we wouldn't put them in an unfortunate situation." (Interviewee 3)

As it was quoted previously, the employees also considered the consequences for people whose information they handle. It was mentioned that one of the reasons to comply with the policies is to protect those individuals from harm.

> "Well one of them is routines, that you just do something when you do it, but it's that – kind of the client's interest is the primary motive for me." (Interviewee 9)

Interviewee 4 also considered the possible consequences the employee or the organization might face in case of a data leak. Interviewee 4 also emphasized his/her personal responsibility and will to protect the customer's information. Interviewee 7 said that one of the motivators is the will to protect their customer's data.

> "I personally wouldn't want my client's information to be public. You could end up in big trouble. – It's something that I want to be able to assure, that the information

> which is in my possession is not used for something it's not meant to." (Interviewee 4)

Two of the interviewees emphasized that they personally wouldn't want to be responsible for a security breach.

> "Obviously it would be terrible, if my carelessness resulted in a security breach or into someone accessing our documents. It would be absolutely horrible if that happened. If the case was that a security breach happened, and you had done everything exactly right, had changed your passwords regularly and had complied with all of the instructions, it wouldn't feel just as bad as it would if you had just been careless. Maybe that's the thing that motivates me to comply with them." (Interviewee 8)

> "Maybe it's just that you don't want to be the person causing something or that you would have to say that something happened because of your own carelessness." (Interviewee 7)

Interviewee 6 also points out the will to behave based on the organization's values. Interviewee 6 considers policies to be just one of the rules they needed to follow, and it is a good practice to work in a secure way.

6.2.4 Summary

In this chapter, the results of the discussions regarding motivation towards ISP compliance were discussed. Table 4 summarizes the factors identified in this chapter. Firstly, the factors of social bonds and social learning were discussed. All the interviewees considered themselves to be somewhat close to at least some of their colleagues. The general atmosphere in the organization was considered trusting and the employer trusts the employees to behave in an expected way. When asked about motivation to comply with the ISP, only one of the interviewees brought up a factor which could be associated with social bond theory. Therefore, although the interviewees had strong social bonds with their colleagues, they did not describe it to be their most substantial motivator.

Regarding social learning, the interviewees considered their attitude towards security to be stricter when they were outside their office. The interviewees brought up that, for example, their colleagues often do not lock their computers when they are working in their office, but they were more cautious about their ways of work and their conversation topics when they were outside the office. It could be argued that the employees were generally accepting less compliant security behavior when they were among each other, thus encouraging each other to act non-compliantly.

From the motivational factors, the obligation towards employer was identified the most often. The interviewees wanted to protect the organization's reputation, the business, its customers and prevent the organization from getting legal consequences regarding GDPR. Some of the interviewees also said that they did not want to be the ones responsible for a security breach in the organization.

Motivational factor	Interviewee
Acting according to organization's values, intention towards expected behavior	Interviewee 6
Maintaining status in work community	Interviewee 7
Maintaining organization's reputation	Interviewee 3
Protecting the business	Interviewee 1, Interviewee 5
Fear of legal consequences	Interviewee 2 Interviewee 8
Protecting the customers and/or the individuals whose information the organization handles	Interviewee 3, Interviewee 4 Interviewee 5 Interviewee 7
Client's interest	Interviewee 9
Fear of being responsible for a security incident	Interviewee 7 Interviewee 8

TABLE 4. Summary of identified motivational factors

6.3 Non-compliance justification

In this subchapter, the second research question, "*What motivates employees to comply with information security policies?*" is discussed. All the interviewees had at least one policy with which they were not complying with. The interviewees were asked to give reasons for not complying with the policies although they knew such policy existed. The interviewees' answers mirrored to the neutralization theory which was introduced in the literature review. Neutralization theory explains, how criminals justify their delinquent behavior with neutralization techniques. (Sykes & Matza, 1957) The aim for neutralization is to justify criminal behavior, or in this case, non-compliant security behavior. Security violations are not criminal behavior as such, but neutralization theory can be applied in this case, as well. (Siponen & Vance, 2010)

6.3.1 Justifying with neutralization techniques

The interviewees were asked what they considered to be the reasons for their non-compliant behavior. While discussing why the work computer is not locked every time employees leave them unattended, interviewee 5 argues:

> "We don't have people coming in to our office who would get in without us noticing, at least not someone who would do something with the information." (Interviewee 5)

This argument can be interpreted as the neutralization technique "The denial of injury". Based on the technique, a criminal justifies the crime by claiming the criminal behavior caused no harm to anyone or the harm was not significant. (Siponen & Vance, 2010) Quite similarly, non-compliant behavior can be justified by a claim that it doesn't cause harm or put the organization at risk. In this comment, it can be observed that the interviewee thinks his/her behavior does not but the organization at risk, which justifies the non-compliant behavior. This neutralization technique was used by other interviewees, as well. In the following quote, the interviewees are not necessary denying the injury, but rather, saying there is no risk of injury. Interviewee 3 ponders that the employees do not know what the risks are and thus, choose not to comply with the policies.

> " I think it's simply because people don't think that something could actually happen from it if I leave my computer open and don't lock it right away. I think it's just about that. -- It hasn't become a habit, and no one can think about what the concrete risks could be." (Interviewee 3)

In the neutralization technique called denial of responsibility, the criminal tries to neutralize the situation by claiming the incident was not on his/her control and tries to put the responsibility elsewhere. Interviewee 3 considers that the topic should have been addressed more when the GDPR came into effect so that the security behavior would have become a habit. The interviewee is moving the responsibility to the others, who should have taken care of the compliance of the employees.

> "I think it's just because nothing has ever happened. Also, when the GDPR came into effect and it was discussed a lot, it should have then been addressed more so that the instructions would've become a habit. " (Interviewee 3)

Interviewee 2 points out that since they have someone in their organization who has been responsible of many security related things, such as GDPR, there is no need for others to familiarize themselves with security.

> "Our x (manager) is kind of the person in charge and that has, in a way, lead myself into feeling that it is someone else's responsibility, so I haven't really had to familiarize myself with it that much, which is probably not the best way to look at things." (Interviewee 2)

Interviewee 9 points out that there has not been much effort made to ensure the compliance of the employees. The interviewee considered that they had only been instructed to read the document, but no follow-up has been made since. The interviewee considered that the organization could have been insisting more from the employees.

> " It's probably that, if I think about how much this has been discussed and what has been insisted, it is just that we have only been instructed to read the document. So, in a way, no noise has been made about it. (Interviewee 9)

This quote could also be interpreted as the neutralization technique "the condemnation of the condemners", in which the criminal blames the ones who are affected by the action to justify his/her behavior. (Siponen & Vance, 2010) In information security context, an employee could justify non-compliant behavior by claiming that the company policies are not reasonable. (Siponen & Vance, 2010) None of the interviewed employees necessarily blamed the organization but criticized it for not addressing the issue enough. Interviewee 3 notes:

> "I think it's just because nothing has ever happened. And, when the GDPR came into effect and it was discussed a lot, it should have then been addressed more so that the instructions would've become a habit. "(Interviewee 3)

The interviewee considers the responsibility to belong to the organization and not just the employees. The interviewee also notes that since nothing has happened before, the employees do not consider there to be any risks. In the example by Siponen and Vance (2010) an employee could argue that the company policies are not reasonable. None of the interviewees brought this viewpoint up, but Interviewee 3 considered that employees should be allowed to make their own judgement and use their common sense to evaluate, which policies need to be strictly complied every time and which do not. Although this is a good point to consider, it can be argued if the employees have the adequate knowledge about security risks to be able to evaluate the necessity of policy compliance. The opportunity to choose whether to comply with the policies can lead an employee to allow non-compliant behavior in situations where compliance would be necessary.

The neutralization technique "Appeal to Higher Loyalties" is based on the idea, that an individual commits a crime in order to resolve or complete something. In a work-context, Siponen and Vance (2010) provide an example of an employee, who violates a policy in order to get his/her work duties done.

> "I'm sure it's just about the prioritization of time, that you'd rather use the couple of seconds or minutes to finish something, rather than prioritize security policies. Maybe, in that moment, you weigh the risks that there is no chance of causing security harms to anyone, although the situation might be different in reality." (Interviewee 2)

This comment might demonstrate the thought process employees may have when facing a situation where they need to choose between being compliant or non-compliant. Prioritizing work duties instead of security practices can be justified with the thought that the organization wants the employees to work efficiently, thus they choose to spend time on work rather than security measures. This, however, is not in the best interest of the company and should be reminded to the employees, as well. The organization could emphasize the value of compliant behavior over productivity. Thus, the employees would not face a situation where they would have to choose.

In the neutralization technique "The denial of the victim", the individual takes responsibility of causing harm, but the action is justified by claiming the target of the crime deserved it or the circumstances of the situation justify the

crime. (Sykes & Matza, 1957) This neutralization technique was not identified from the interview results and it was one of the most difficult techniques to evaluate in this context where no crime or violation has been done. None of the interviewed employees showed malicious intentions towards their organization. Therefore, none of the interviewees would justify their non-compliant behavior based on circumstances or consider the organization to somehow deserve that kind of behavior. Therefore, the technique "The Denial of the Victim" was not identified in this study. In Table 5, the identified neutralization techniques are summarized.

Neutralization technique	Interviewee
The Denial of Responsibility	Interviewee 2, Interviewee 3, Interviewee 9
The Denial of Injury	Interviewee 3, Interviewee 5
The Denial of the Victim	No observations
The Condemnation of the Condemners	Interviewee 9
The Appeal to Higher Loyalties	Interviewee 2

TABLE 5. Summary of identified Neutralization techniques

6.3.2 Other findings

Besides the neutralization techniques, other justification methods were identified from the interviews. Interviewee 9 emphasized the secure atmosphere of the organization and the feeling of trust which can lead into a thought that it is not necessary to comply with the security policies.

> "I've always had a job where the atmosphere is very relaxed, and the doors have been kept open, so it probably creates such a secure atmosphere, which can falsely lead into a convivial attitude." (Interviewee 9)

Perception of risk was also discussed earlier in this paper. Interviewee 7 said that (s)he does not consider there to be any risk if the passwords are not changed. Thus, (s)he has not found changing passwords necessary. This finding would suggest that the employees have no knowledge of the possible consequences of not following the security instructions.

> "I just haven't thought that there would be any kind of risk if I didn't change them (passwords)." (Interviewee 7)

While discussing the organization's efforts towards security and the interviewee's thoughts towards security, Interviewee 9 notes:

> "I think the reason why I don't think it that much is, at least from my perspective and probably from others as well, is because we have a scheme of things that everyone carries the responsibility of their own actions. Therefore, we don't do things based on how we have been instructed to do things but based on what is in the best interest of the company. For me, it is easy to comply with the instructions because I understand the reasons behind them and kind of the whole picture. What it says in the policy, I myself don't find it that essential. As long as you understand where the risks are, where the information can get into wrong tracks, where someone can access the information and avoid those situations, you don't need instructions for that." (Interviewee 9)

Although trusting the employees to do the right thing creates trust between employees and employer, it does not deny the fact that all the employees do not have the same knowledge about security. Therefore, security instructions need to shared and mutual with every person in the organization and the employees need to be educated why such instructions are taken in place. Those employees, who are experienced in security might not have to be reminded of the policies but as in this organization most of the employees are not experiences, they need to be educated and required to act compliantly.

Interviewees 6 and 8 said that the reason why they have not changed their passwords is purely because they have not remembered to. Interviewee 6 considered the possibility of having someone reminding them to change their passwords or having an automatic reminder. The policy does not specify, how often the passwords should be changed but the interviewees thought that there should be a common rule for changing the passwords, which would be reminded.

> "I just haven't remembered to. It has not never crossed my mind. Maybe I should have a reminder for myself so that I would remember to change my passwords." (Interviewee 6)

Interviewee 8 also considered that since changing passwords is such a small task, it is easily overridden by other tasks. For both indolence and forgetfulness, regular reminders might help the employees to take time for changing the passwords.

> "I think it's only because of my own laziness and forgetfulness. You kind of think that it's such a small thing, that you would rather do other things and come back to it (changing passwords) later and then you forget about it. (Interviewee 8)

Interviewee 7 points out the inconvenience of changing passwords often, as they are then easily forgotten, as well. Interviewee 7 justifies not changing the passwords by the effort it would require.

> "I'm sure that someone might misuse them (passwords) if they got access to them, but it's just something that I'm pissed about, that you need to have passwords eve-

> rywhere. If you had to change them every month, I would constantly have to be resetting my passwords because I'd forgot them." (Interviewee 7)

Similar answer was given by Interviewee 1, who considered that since there are so many passwords they need to remember, changing passwords would mess their password logic and would result in a "mess". The use of password mangers was discussed, but the interviewee said to not be comfortable with using them. However, password managers would help the employees to store their passwords and make changing them easier as you would only have to remember the master password. Password managers also enables the use of more complex passwords.

Interviewee 2 says that (s)he is not overly cautious about security, because (s)he thinks that everyone wants to keep the organization's information with themselves and there is no risk for harm to happen.

> "In a way, it's the unawareness. And you also think that everyone thinks the same way you do, that since you've written a contract, you're committed to keeping things inside the walls of our organization or with yourself and that's probably why you trust too much that it is how you all behave." (Interviewee 2)

In the discussion of locking computers, Interviewee 4 said that since they have very little people in their office and they know each other well, they trust each other so much that they do not worry about locking their computers every time. Therefore, trusting your colleagues can be a way to justify non-compliant behavior, as the employee might not consider his/her colleagues to be a threat.

> "I'm sure it's related to the fact that we have the same regular people and very little people in our office, people know each other personally which creates trust." (Interviewee 4)

6.3.3 Summary

In this chapter, the strategies interviewees used to justify their ISP violations were discussed. In Table 6, the identified justification strategies are presented. The table first presents the identified neutralization techniques and then the other identified strategies.

One of the main theories observed in this chapter was the neutralization theory. All except one of the neutralization techniques were used by the interviewees. The most used technique as the technique "The denial of the responsibility". This technique is used in situations where the employee claims the incident was not on his/her hands and the responsibility of the violation is given to someone else. The second most used technique was "The denial of injury" which justifies the behavior by claiming the violation does not cause harm to anyone. The neutralization technique "The denial of the victim" was not identified in this study.

With other justification techniques, there were more dispersion. One of the interviewees considered forgetting instructions such as changing passwords to be the reason for non-compliance. Two of the interviewees considered some of the policies to be inconvenient to execute. Two of the interviewees considered there is no risk for a security threat, hence they did not find compliance necessary. One of the interviewees admitted indolence to be the reason for non-compliance. Finally, two interviewees said that since they feel like they can trust their colleagues they do not need to pay that much attention to policies such as locking your computer or changing passwords.

Justification	**Interviewee**
Neutralization techniques	
The Denial of Responsibility	Interviewee 2, Interviewee 3, Interviewee 9
The Denial of Injury	Interviewee 3, Interviewee 5
The Denial of the Victim	No observations
The Condemnation of the Condemners	Interviewee 9
The Appeal to Higher Loyalties	Interviewee 2
Other identified justification strategies	
Forgetfulness	Interviewee 6
Inconvenience	Interviewee 1 Interviewee 7
Perception of risk	Interviewee 2 Interviewee 7
Indolence	Interviewee 8
Trusting colleagues	Interviewee 2 Interviewee 4

TABLE 6. Summary of identified justification strategies

7 DISCUSSION

Employees' security behavior can have a major effect in the organization's overall level of information security. In this thesis, the literature review was conducted to observe the different factors which had been identified to affect employees' security behavior. In the empirical study, the employees' own perception of their security behavior, their motivation to comply with organization's security policies and justifications for non-compliance were observed through a case study. The themes for the interviews were built based on the themes found from the literature review. Thus, in this chapter, the results of the empirical study are compared to the findings of the literature review. Also, the new findings are discussed.

This chapter aims to answer the two research questions for this study: "*What motivates employees to comply with information security policies?* and "*How employees justify their non-compliant ISP behavior?*". In subchapter 7.1. the findings of the study are discussed. In subchapter 7.2. the limitations of this study are discussed and in subchapter 7.3. the suggestions for further study are made.

7.1 Discussing the findings

In this subchapter, the findings from the study are further discussed. This subchapter will follow the same structure as the results chapter, which means that the discussion will follow the identified and described themes. Firstly, the interviewees' perception of ISP compliance and their actual security behavior is discussed. Secondly, the reasons interviewees gave for complying with ISP's are discussed. Thirdly, the neutralization strategies interviewees used to justify ISP violations are addressed and compared to the findings of the literature review.

7.1.1 ISP compliance vs. actual security behavior

One of the major findings of the interviews was that although the interviewees considered themselves to be complying with the organization's ISP, their actual security behavior proved otherwise. Several different speculations can be made from this finding. Many of the interviewees had read the policy a long time ago and it is possible that they did not recall the contents of the policy. For this scenario, it would be important that the organization would regularly remind the employees of the policy or have regular training sessions of the topic. It is also possible that the interviewees genuinely believer their security behavior is compliant, and they thought they had been behaving as expected even though it was not the case. Also, in this scenario, the organization should pay attention to the employees' actual behavior and remind them of possible non-compliant behavior. Auditing measures could also take place.

It was brought up in the interviews that the organization trusts the employees' security behavior to be compliant, thus the actual behavior is not regularly monitored. Many of the interviewees felt that monitoring and notifying employees could help remembering the policies, but it should be coherent and the responsibility for monitoring should not be on the shoulders of one employee. In an organization where the employees work in different offices and often remotely monitoring would be challenging.

Another theme included in this chapter was the interviewees' perception of security risk. Most of the interviewees considered that it was likely that the organization could face a security threat of some kind. Only two of the interviewees considered there were no risk. As an interesting observation, it was observed if there was a connection between employees' perceived risk and actual security behavior. Surprisingly, there was no clear connection. Although those interviewees who considered there to be no risk also complied less with the policies, some of those interviewees who did consider there to be a risk of a security threat also admitted not complying with most of the policies. Therefore, no straightforward conclusions can be made from this finding and to prove a connection further studies should be made.

However, the discussion of perceived risk showed that the interviewees had no knowledge about the risks their non-compliant behavior can result in. Although the interviewees considered that as their organization has been growing and gaining publicity, their organization could be a target for someone they did not consider how their own security behavior could enable such security threats. It was brought up later in the study, that some of the interviewees justified their non-compliant security behavior with the thought that they can trust their colleagues and the people visiting their office. This line of thought does not take into consideration the possibility of insider threat and the risks the organization's own employees might pose. It also needs to be considered that, for example, never changing passwords can give a slot for an external intruder to attack the organization.

This connection between perceived risk and actual behavior needs to be addressed. As most of the interviewees had no background in information security, it is understandable that they do not have all the knowledge about possible risks. The responsibility of sharing such knowledge is with the employer. When the ISP is introduced, it would be beneficial for the organization to present the possible outcomes of non-compliant behavior. Through understanding the reasons for the policies, the employees may be more likely to comply with the policies.

7.1.2 Motivation for compliance

The first research question aims to find answers to what employees themselves consider to be their motivator to comply with the organization's information security policies. Regarding interviewees' motivation towards ISP compliance, similar factors were identified from both the literature review and the empirical study, but some differences were identified, as well. Social bonds and social learning were difficult themes to observe. Although the interviewees considered themselves to be close with their colleagues, none of the interviewees mentioned social bonds to be their motivator for compliant behavior. One of the interviewees considered that s(he) would not want to be the one to cause trouble for the organization which suggests that the interviewee wanted to maintain his/her status in the work community. It could be argued that social constructs and effects of social environment can be difficult to recognize, which could be the reason for the small amount of observations of social factors.

Social learning was not directly addressed by any of the interviewees. However, it was brought up in the interviews that the general way of acting in the organization was that the employees were less cautious inside the office than outside the office. General approval for such behavior could influence the employees, as the social learning theory suggests that the observations employee makes from his/her surroundings can affect the perception employee has of accepted behavior. (Theoharidou et al. 2005) Thus, if all the other employees tend to have a less strict attitude towards security, it might affect the attitude of the employee, as well.

The interviewees' thoughts about punishment as a motivator was discussed. General deterrence theory states that an individual is less likely to engage in criminal activity if there is a possibility of sanctions. (D'Arcy & Herath, 2011) General deterrence theory was difficult to identify from the results as the case organization does not currently give sanctions for non-compliant behavior. More specifically, the security behavior is not monitored at all at the moment, which would make giving sanctions difficult. Most of the interviewees did not consider the idea of deploying sanctions in the organization pleasant, but some of the interviewees mentioned that giving sanctions might be an effective way to assure compliance. Monitoring employees and giving sanctions for non-compliant behavior was considered to negatively impact the general atmosphere of the organization. It was also discussed that it would put the person in

charge of security to an unpleasant position. It was suggested that non-compliant behavior should be pointed out and the employees should be reminded of the policies in a constructive way. On the contrary, the attitudes towards rewarding were discussed. Many of the interviewees considered that rewarding for compliant behavior would be a better approach in this organization rather than giving sanctions.

One interesting finding was that many of the interviews did not want to cause any trouble for the organization. In these discussions, the GDPR was brought up many times. After GDPR came into effect, the employees have had to consider the legal consequences which may occur if the regulation is violated. Many of the interviewees brought up that they would not want to cause the organization any legal trouble and thus wanted to ensure they were acting as they were expected. It was also an interesting finding regarding the fear of sanctions, that the interviewees considered legal consequences to be a major motivator. Thus, it could be argued that fear of sanctions does have an impact on the behavior of the employees. Following the same line of thought, having internal sanctions could influence the employees' attitude, as well. However, it would be difficult to separate if external sanctions would be more effective than internal ones. This would need to be studied further to make any conclusions.

A significant finding was that many of the interviewees considered obligation towards employer to be their biggest motivator. It was, in many occasions, emphasized that the organization trusts its employees and the employees liked to work in the organization. These factors could have an impact of the interviewees' experience of obligation towards the employer. This view would be supported by Leach (2003) who found in his study that the employees who are satisfied with how they are being treated at work usually feel more obliged to their employee and thus feel the pressure to behave as expected.

One of the findings regarding obligation towards employer was the interviewees' intention to maintain the organization's business and reputation. Maintaining reputation can be a major factor for the organization's business as security leaks can cause extensive losses for the organization as negative publicity can withdraw customers and stakeholders. (Cavusoglu et al. 2004) This point of view was brought up in many of the interviews and the interviewees mentioned that when GDPR came into effect, they had had many training sessions and the topic was often discussed. This finding would suggest that regular trainings and keeping the discussion up about security might encourage the employees to be more compliant.

There were also factors which were not identified in the literature review. In Table 6, the factors identified in the literature review and in the empirical study are compared. One of the factors not identified in the literature review was protecting their customer's and customer's customers' personal information. The interviewees did not want to cause mischief for people whose personal information they were collecting and handling. Another identified motivator was that the interviewees did not want personally to be the ones who have caused a security incident.

Some of the factors identified in the literature review were difficult to observe from the empirical study. For example, organization's security environment which was suggested by Leach (2003), Banerjee et al. (1998) and Vroom & von Solms (2004). The interviewees did consider their organization to be somewhat invested in security but also considered that the organization could pay attention to it more. The organization had been investing in security especially when GDPR came into effect but as the topic became less urgent, the company was not putting that much effort into it. It would be difficult to evaluate, to what extent the organization's security environment has affected the motives of the employees, but as there were no clear evidence of such connection, no such conclusion was made. Also, quality of company policies (Leach, 2003; Pahnila et al., 2007) was not observed as a motivational factor in the empirical study.

Identified motivational factor	Literature review	Empirical study
Intention towards expected behavior	X	
Social bonds	X	X
Social learning	X	
Risk of sanctions (legal consequences)	X	X
Obligation towards employer	X	X
Perceived risk	X	
Exemplary behavior of managers	X	X
Security environment	X	
Quality of company policies	X	
Fear of being responsible for security incident		X
Protecting the individuals whose information is handled		X
Client's interest		X
Protecting the reputation and business		X

TABLE 6 Summary of identified motivational factors in literature review vs. in empirical study

7.1.3 Non-compliance justification

The second research question aims to find the strategies employees use to justify their non-compliant security behavior. As well as with the first research question, there were some similarities identified between the literature review and the empirical study, but some differences were identified, as well. The main neutralization strategies employees used to justify violating the security requirements were contrasted to neutralization theory, but other justification strategies were identified, as well. Firstly, the identified neutralization techniques are discussed and contrasted to the literature review. Secondly, other

justification strategies which were not identified in the literature review are discussed.

The identified neutralization techniques were the denial of responsibility, the denial of injury, the condemnation of the condemners and the appeal to higher loyalties. The neutralization technique of the denial of the victim was not identified in the empirical study. These neutralization techniques had been studied in the studies by Sykes & Matza (1957) and Siponen & Vance (2010) The most used neutralization technique was the denial of injury, where the employee considers that no harm is done if security policies are violated. The denial of injury can be linked to the employees' perception of risk and the possible consequences security violations might result in. The employee might consider that not paying attention to security instructions does no harm to the organization, although the case is quite the opposite. Again, the importance of educating the employees about the possible risks and outcomes which might occur for non-compliant security behavior.

The neutralization technique, the denial of responsibility was identified in situations where the interviewee was putting the responsibility on the organization. In these situations, the interviewee considered that the organization should have put more effort on the education of the employees as well as on the follow-up after the ISP was introduces. Also, it was brought up that since the organization had someone taking care of GDPR related issues, some interviewees considered the responsibility of security to be with that person. Therefore, some considered security to be handled by someone else, although security is something everyone needs to pay attention to in order to be effective. However, having someone else taking care of security, it can falsely lead into a conception that no efforts is needed to strengthen security.

The neutralization technique of the condemnation of the condemner was not identified in many of the interviews. This technique was brought up as criticizing the organization for not addressing the importance of ISP compliance. None of the interviewees suggested that the organization was to blame for non-compliant behavior, but they considered the organization should have been focusing on it more. The neutralization technique, appeal to higher loyalties, was also identified. As Siponen and Vance (2010) suggested, an example of this technique could be about an employee who violates security policies to get work done faster. The same example was brought up by some of the interviewees. This would suggest that security measures should be accomplishable fast and easy, and they should be formed into a routine which the employee can do without the task taking too much time and effort.

Another factor identified from the literature review was security knowledge which had been studied by Leach (2003) and Hazari et al. (2008). Security knowledge was a difficult factor to observe but as it can be observed from this discussion section, education has a major impact in the security behavior of employees. Security knowledge would improve the employees' perception of risk and the general knowledge about which measures can be and should be taken against to protect the organization from those risks. In the liter-

ature, security knowledge had been found to improve the security behavior of employees. However, in this study the finding is a bit inverse. It can be argued, that the lack of security knowledge negatively affects the security behavior.

All factors identified in the literature review, except the neutralization technique the denial of victim, were identified in the empirical study. However, some other factors were identified as well. Those factors are forgetfulness, inconvenience, indolence and trust towards colleagues. Forgetfulness was identified from interviewees, who thought the biggest reason they did not comply with the policies is that they did not remember them. Especially the policy for changing passwords was considered difficult to apply and the interviewees considered they should have a regular reminder for changing them. Another factor related to forgetting was the inconvenience of putting policies intro practice. Especially changing the passwords and locking the computer were considered inconvenient and difficult to apply. Indolence was also identified and some of the interviewees felt that it was often easier to not apply security policies and to carry on with other tasks which feel more important at that moment.

The last identified factor was trust towards colleagues. It was discussed that since other employees can be trusted, some security measures, such as locking the computer, do not need to be so strictly complied. However, an insider with malicious intentions can take advantage of such trust and can result in a security violation. Also, there is a possibility that an intruder with malicious intentions can have access to the office of the organization and can that way take advantage of negligent behavior.

To summarize the findings of this chapter, it can be said that almost all the strategies identified in the literature review were also identified in the empirical study. The justification strategies identified in the literature review were compared to the results of the empirical study in table 7. The identified strategies were the denial of responsibility, the denial of injury, the condemnation of condemners, the appeal to higher loyalties, perception of risk and security knowledge. In addition to these findings, also other justification strategies were identified, which were forgetfulness, inconvenience, indolence and trust towards colleagues.

Justification strategy	**Literature review**	**Empirical study**
The Denial of Responsibility	X	X
The Denial of Injury	X	X
The Denial of the Victim	X	
The Condemnation of the Condemners	X	X
The Appeal to Higher Loyalties	X	X
Forgetfulness		X
Inconvenience		X
Perception of risk	X	X
Indolence		X

Trust towards colleagues		X
Security knowledge	X	X

TABLE 7 Justification strategies identified in the literature review compared to the results of the empirical study

7.2 Limitations of the study

In this subchapter, the limitations of this study are discussed. As in every study, also this study had limitations which may have affected the reliability and generalizability of this study. The identified limitations were related to the single-case study, the sampling size, the researcher and possible biases.

The first limitation of this study is that the research was conducted as a single case study in one organization. Conducting a multiple case study could have resulted in more extensive and variable results. Selecting only a one case also means that there is no comparison material, which can result in unilateral results. As the organization operates in a small area of the business and is a small organization, the culture of the organization might differ from bigger corporations. Therefore, when observing the results of the study it should be considered that the results may not be generalizable.

The second limitation of the study is the size of sampling of this study. The amount of the interviewees was rather small, which could have affected the generalizability of the results. Although there is no definition for suitable research sample size in qualitative research, more interviewees could have resulted in more generalizable results. However, if the total number of employees in the case organization is considered, the sampling was enough compared to that.

The third limitation is related to the researcher. The researcher is inexperienced as this study has been the first empirical study the researcher has conducted. This might have affected many parts of this study, from conducting the interviews to analyzing the results. Also, although the researcher had been conducting literature reviews before, searching for and limiting the chosen papers for this study might have left some papers out of this study.

The fourth limitation is the possible biases of the interviews. Due to the inexperience of the researcher, it is possible that the interviews were not fully neutral or essential questions were left out. As the interviewees were not very familiar with the research topic, the researched had to steer the interviews which may have affected the answers and results of the interviews. Although the interviews were transcribed word-to-word, there is always a possibility that the subjective interpretations of the interviewee may have affected the analysis of the interview data. To avoid possible biases, the interviews were conducted as semi-structured interviews which helped to form the questions neutrally.

7.3 Suggestions for further study

In this study, the organization had introduced the ISP one year before the interviews. It would have been interesting to study the case organization as a longitudinal study, where the employees would have been interviewed before the deployment of a new security policy and again a couple of months after the deployment. By conducting a longitudinal study, the intention for certain security behavior and justifications for non-compliance could have been better observed.

Another suggestion for further study would be conducting the same study with a bigger sampling. Bigger sampling could have been beneficial for the results of the study, maybe even having a multiple case study would have led into different and more generalizable results. Another topic for future research would be observing the differences between compliance of organization's internal policies and external regulations, such as GDPR. Observing how these different guidelines are complied with would be an interesting topic for future research.

8 CONCLUSIONS

The aim for this Master's Thesis was to identify the factors, which affect employees' ISP compliance and behavior. The research questions for this study were "*What motivates employees to comply with information security policies?*" and "*How employees justify their non-compliant information security behavior?*". These themes were studied through a literature review and an empirical study. The empirical study was conducted as a qualitative case study in a Finland-based organization and the interviews were conducted as semi-structured interviews. The interview was constructed based on themes identified in the literature review. As current organizations are relying on technology and digital tools, the importance of maintaining security is crucial. One of the biggest factors in maintaining security is the security behavior of employees, hence the factors affecting their security behavior need to be identified. This study and its results are important for organizations to help them identify, how organizations can support their employees to be more compliant.

In the second chapter of this study, the main concepts of this study are identified, including insider threat and classification of security threats. In the third chapter, the relevant theories regarding this study are presented and discussed. The fourth chapter summarizes the literature review. The fifth chapter describes the research method for empirical study and the scope of the study. In the sixth chapter, the results of the empirical study are discussed. In the seventh chapter, the results are discussed and analyzed. The final chapter of this study concludes the study.

This study aimed to find answers for the defined research questions by conducting literature review and an empirical study. The empirical study was based on the findings of the literature review and the papers included in the literature review provided a broad view of the topic. The empirical study followed the findings of the literature review to some extent, but new findings were made as well. It needs to be reminded that a qualitative case study might not provide generalizable findings but nevertheless, the findings of the study provide an interesting visual angle to the thoughts of employees.

For the empirical study, 9 employees of a Finnish-based organization operating in B2B were interviewed. As the sampling for this study was quite small, the findings of the study are not generalizable, but they address the difficulty of defining and predicting human behavior. For this study to be more generalizable, more companies could have been interviewed to get a broader viewpoint of the topic.

These research questions were answered by observing three different themes: employees' perception of security behavior versus their actual behavior, motivational factors to comply with organization's ISP and justification strategies to justify non-compliant security behavior. As an answer for the first research question about the motivational factors, it was observed that the most general factors were protecting the individuals whose information the organization handles, protecting the business and its reputation, risk of legal consequences, and fear of causing security incident. One of the main findings for the first research question was the interviewees' obligation towards their employer and the will to protect the organization and its customers. This finding suggests that if the organization puts an effort on having committed and obliged employees, they are more likely to protect the organization and follow the organization's ISP. For the second research question, the most used justification strategies were identified to be the denial of responsibility, the denial of injury, inconvenience, perception of risk and trust towards colleagues. The findings for the second research question emphasizes the importance of educating employees of the possible risks and the possible consequences of non-compliant behavior.

Although there were many similarities in the findings of the empirical study and the literature review, also differences were observed. For the first research question, the literature review identified factors such as intention towards expected behavior, social learning, perceived risk, security environment and quality of policies, which were not identified in the empirical study. For the second research question, only one of the strategies identified in the empirical study was not identified. This strategy was the neutralization technique "The Denial of the Victim". This finding also underlines the interviewees' obligation towards the organization, as none of the interviewees considered the organization to deserve the harm their non-compliant behavior might cause.

As the sampling for this study was rather small, the results of the study might provide a narrow viewpoint which may not be generalizable to other organizations. There were also some differences between the findings of the literature review and the empirical study, which would make a further study with a bigger sampling and multiple case organization an interesting study to conduct. It would also be interesting to investigate further, if there are differences with the motivational factors to comply with the organization's internal policies and external regulations, such as GDPR. Observing how these different guidelines are complied with would be an interesting topic for future research.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Alasuutari, P. (2012). Laadullinen tutkimus 2.0. Tampere: Vastapaino. E-kirja.

Aytes, K., & Conolly, T. (2003). A research model for investigating human behavior related to computer security. *AMCIS 2003 Proceedings*, 260.

Bandura, A., & Walters, R. H. (1977). *Social learning theory* (Vol. 1). Englewood Cliffs, NJ: Prentice-hall.

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT ethics: A study in situational ethics. Mis Quarterly, 31-60.

Basit, T. (2003). Manual or electronic? The role of coding in qualitative data analysis. *Educational research*, *45*(2), 143-154.

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337-346.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151-164.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Burnard, P. (1991). A method of analysing interview transcripts in qualitative research. *Nurse education today*, *11*(6), 461-466.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of ITSecurity Management: Four Improvements to Current Security Practices. Communications of the Association for Information Systems, 14(1), 3.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security*, *1*(3), 18-41.

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345-361.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188.

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

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

Eisenhardt, K.M. (1989). Building theories from case study resarch. *Academy of management review, 14(4),* 532-550.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*(2-3), 203-225.

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, *111*(7).

GDPR Key Changes, EU GDPR.org, retrieved 09.05.2019 from https://eugdpr.org/the-regulation/

Gonzalez, J. J., & Sawicka, A. (2002, October). A framework for human factors in information security. In *Wseas international conference on information security, Rio de Janeiro* (pp. 448-187).

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. IEEE Security & Privacy, 6(1).

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242-251.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems*, *28*(2), 203-236.

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security*, *4*(4), 3-20.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hirschi, T. (1969). Causes of Delinquency University of California Press. Berkeley, CA.

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. European Journal of Information Systems, 18(2), 140-150.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. Information Systems Research, 26(2), 282-300.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, *54*(6), 54-60.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. Computers & Security, 21(5), 402-409.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69-79.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *36*(4), 68-79.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. International journal of information management, 23(2), 139-154.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049-1092.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685-692.

Leonard, L. N., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived

importance, or individual characteristics?. *Information & Management*, *42*(1), 143-158.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. MIS quarterly, 71-90.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly*, 173-186.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. Information Resources Management Journal (IRMJ), 24(3), 1-8.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). TOWARD A UNIFIED MODEL OF INFORMATION SECURITY POLICY COMPLIANCE. *MIS Quarterly*, *42*(1).

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on (pp. 156b-156b). IEEE.

Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users?. *Information Management & Computer Security*, *15*(5), 362-371.

Peltier, T. R. (2006). Social engineering: concepts and solutions. *Information Security Journal*, *15*(5), 13.

Posey, C., Roberts, T., Lowry, P., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816-826.

Sarajärvi, A., & Tuomi, J. (2017). *Laadullinen tutkimus ja sisällönanalyysi: Uudistettu laitos*. Tammi.

Saaranen-Kauppinen & Puusniekka. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto. Retrieved 30.05.2019 from http://www.fsd.uta.fi/menetelmaopetus

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526-531.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38(1), 60-80.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & security, 24(2), 124-133.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS quarterly, 441-469.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24(6), 472-484

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167-173.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, 18(2), 101-105.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816.