Kimmo Rantonen

EXPLAINING INFORMATION SECURITY BEHAVIOR – CASE OF THE HOME USER

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2014

TIIVISTELMÄ

Rantonen, Kimmo
Kotikäyttäjien tietoturvakäyttäytyminen
Jyväskylä: Jyväskylän yliopisto, 2014, 58 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Tässä pro gradu – tutkielmassa tutkittiin kotikäyttäjien tietoturvakäyttäytymistä. Mitkä tekijät vaikuttavat tietoturvakäyttäytymiseen, miksi tiettyjä suojakeinoja omaksutaan ja toisia sivuutetaan? On väitetty että kotikäyttäjät voivat olla uhka niin itselleen, muille kuin koko kyber- infrastruktuurille. Tutkielmassa hyödynnettiin kirjallisuuskatsausta sekä haastatteluja vastausten saamiseksi.

Kirjallisuuskatsauksen perusteella voidaan päätellä, että kotikäyttäjien käyttäytymiseen vaikuttaa uhan tunteen vakavuus sekä todennäköisyys mutta reagointi uhkaavaan tilanteeseen riippuu myös yksilön atk-taidoista sekä itseluottamuksesta (minäpystyvyys). Yleisesti paremmat taidot johtavat korkeampaan tietoturvaan. Käyttäjien asenteisiin vaikuttamalla tuloksia voidaan myös saada. Lopuksi, ystävien ja tuttujen neuvot sekä median vaikutus ts. subjektiiviset normit voivat myös vaikuttaa positiivisesti tietotoruvakäyttäytymiseen.

Haastattelut tukivat suurelta osin olemassa olevaa kirjallisuutta mutta esille tuli myös uutta käsitteistöä aihepiiriin liittyen. Haastatteluiden perusteella voidaan väittää mm., että käyttäjät laiminlyövät tietoturvaa jos oma tieto nähdään arvottomana. Tietoturvaa voidaan parantaa pakottamalla tiettyjä tietoturva käytänteitä sekä suosimalla automaatiota. Kun käyttäjä saa itse päättää käytettävistä keinoista, tietoturva yleensä heikkenee. Huonot kokemukset saavat uhan tuntumaan oikealta ja siten parantaa myös tietoturvaa. Huonojen kokemusten jälkeen uhka ei tunnu enää teoreettiselta ajatukselta vaan vaara koetaan oikeaksi. Ulkoiset vaikutukset kuten neuvot ystäviltä ja tuttavilta sekä mediasta tulevat varoitukset ja kehotukset vaikuttavat käyttäjiin positiivisesti. Lopuksi, haastatteluiden perusteella atk-taidot johtavat parempaan tietoturvaan mutta eivät aina, koska tietyissä tilanteissa ylimielisyyttä käytänteitä kohtaan voi esiintyä. Vähemmän taitavat käyttäjät laiminlyövät tietoturvaa useasti koska heillä ei ole tarvittavaa tietämystä erilaisista uhista.

Lopussa tutkielman tuloksia ja niiden vaikutuksia pohdittiin suhteessa olemassa olevaan kirjallisuuteen sekä tuleviin tutkimuksiin. Tuloksia myös pohdittiin käytännön näkökulmasta.

Asiasanat: tietoturvakäyttäytyminen, asenteet, kotikäyttäjä, minäpystyvyys, subjektiiviset normit,

ABSTRACT

Rantonen, Kimmo
Explaining user information security behavior – case of the home user
Jyväskylä: University of Jyväskylä, 2014, 58 p.
Information Systems, Master's Thesis
Supervisor(s): Siponen, Mikko

This thesis set out to understand more about the phenomenon of home user information security behavior, what factors influence home user behavior and why some safety measures are adopted while others dismissed. It has been claimed that this big and growing group of users can be a threat to themselves, others and the whole cyber infrastructure. Thesis was implemented by reading relevant literature and conducting interviews to a small group of home users.

Based on the literature, it was discovered that home users are influenced when security threats are seen as real and severe (threat appraisal) but influence works better if the individuals have the necessary skills and confidence (i.e. self efficacy) to react to these threats. In general better computer skills tend to lead to higher information security. By influencing users' attitudes, better information security can also be achieved. Finally, advices and suggestions from friends and peers as well as media visibility, i.e. subjective norms are seen as influencing factor on home user information security behavior.

Interviews mostly confirmed the existing literature but also brought up some new concepts to discussion. Based on the data some claims can be made about the home user's information security behavior. First, users tend to neglect security when information is seen as invaluable. Second, information security can be improved when safety measures are forced on the users or if they are automatic in nature and giving the choice (whether to activate a safety feature) to the home users seemed to result in lesser security. Third, bad experiences work as a good tool to enhance threat appraisal therefore improving security. Such experiences make threats look very real and protection is not something theoretical to the user anymore. Fourth, external influence from peers, family and various medias influence users in a positive way. Finally, in the interviews it was found that skills lead to better security yet not always as some overconfidence might develop. Less skilled users seem to neglect some information security due to lack of knowledge about different threats.

In the end of the thesis implications to research and practice where discussed to point out contributions of the study.

Keywords: Information security behavior, home user, threat appraisal, self efficacy, attitudes, subjective norms

TABLE OF CONTENTS

1 USER – THE WEAKEST LINK IN INFORMATION SECURITY

The use of internet is growing, more and more individuals use the internet on daily basis. According to a recent study, in Finland 87% in the age group of 16-89 use the internet and the frequency of use have been growing in recent years (SVT, 2014). Use of the internet is also diversifying as Finns are increasingly using the web for internet banking, shopping, social networking and not just with their computers but with their phones and tablet computers as well. While internet brings all kinds of benefits to users there is a downside to it all. Information security threats await the unsuspecting users.

The role of the user in information security is a growing concern in both the workplace and in home context. In research, users have been characterized as the "weakest link" in information security. Such characterization refers to poor skills and neglect people represent on information security matters for example in workplace or downright malicious abuse of confidential information by the employees. Indeed, in the organization setting much research has been conducted to explain how employees would follow set rules and guidelines better and how insider threats could be prevented. Such research stream in literature has been called as information security behavior research. In home context there is limited understanding to how users could be influenced and what drives people to behave in secure manner (Agarwal & Anderson, 2010). While research of the topic exists in the workplace, there are differences to home use context and for this reason differences should be acknowledged for the research to develop (Li & Siponen, 2011). This thesis is interested in the information security behavior of individuals, both in the workplace and in home context. While organizational research on the topic works as a foundation, the core of the thesis is in home user information behavior.

There are important reasons to why home user information security behavior should be researched more. First, both in Finland and globally the number of internet users is massive and ever growing. Such a big group of people can be a risk to themselves and to the whole internet. Unlike employees, home users don't usually receive any training on information security matters and

there is no it-support either in case something goes wrong (Agarwal & Anderson, 2010). Therefore these home users can be vulnerable to the threats of the internet. Although citizen safety on the internet is important the ramifications can exceed beyond individual targets. It has been noted that the behavior of the general public can jeopardize other internet user as well as organizations and in worst case, confidence of conducting business or individual transactions over the internet can deteriorate if the stability and security of the cyber infrastructure is compromised (Anderson & Agarwal, 2010). So in keeping the individuals and the whole internet safe, it is important to know how home user information security behavior on the internet can be influenced.

1.1 Research questions and methods

The purpose of the thesis is to find out the factors that influence home users information security behavior. Why users adopt some of the safety precautions and dismiss others? The research will shed light on subjects such as why some protective measures are dismissed. Is this due to poor IT skills and lack of knowledge on security related issues or are home users just lazy? The idea is to also extend the research on devices such as smartphones and tablet computers to see if there is any difference between information security behavior on home computers and mobile devices. Answers to the research questions are acquired via literature review on the subject as well as organizing semi structured interviews to a small group of home users. The purpose of the study can be summed up to two questions:

- What factors influence home user information security behavior?
- Why users adopt some of the safety precautions while dismissing others?

1.2 Structure of the thesis

The rest of the document is as follows. First, the concept of information security itself is introduced and discussed to clarify the background of the topic. Also, in the same chapter the context of the thesis, "home user information security behavior" is defined. Point here is to clarify what kind of behavior is considered as "home user information security behavior" in this particular thesis. Chapter three consists of overview about the research that has been conducted in the workplace context. Many of the relevant theories to home user research can be traced to the organizational research stream. Chapter four focuses on the research that has been done in the home user context.

In chapter five the used research methods for the empirical part of the study are first outlined and justified. In the same chapter the actual research setting is described to give information about who were interviewed and how.

Chapter aims to clarify what kinds of methods are used so that relevant data to the research questions could be acquired. In chapter six the content of the interviews is analyzed and the seventh chapter discusses the main findings and implications of the conducted research. Finally chapter eight concludes the thesis and answers what was researched and why, and what was found in the study.

2 INTRODUCTION TO INFORMATION SECURITY

In this chapter the concept of information security, often shortened to "infosec", is discussed. Based on the literature an understanding of the term information security is established. In order to understand information security behavior it is important to know what infosec actually means. Chapter works well as an introduction to the field of infosec as some key concepts are discussed in detail. Finally the topic of information security behavior in the home user context is clarified to describe what exactly is being studied in this thesis.

2.1 Information security - definitions and key concepts

To put it simply, information security is about the protection of information. In "principles of information security" Mattord and Whitman (2012) defines information security as: "The protection of information and the systems and hardware that use, store, and transmit that information." (Mattord & Whitman, 2012, 588). Similar but in business context, ISO 17799 standard defines information security as protection of information, but here information security has a role in ensuring business continuity, minimizing business risk, maximizing return on investments and business opportunities (ISO 17799).

Quite often, when talking about information security, three characteristics of information are presented. These characteristics of information are confidentiality, integrity and availability, also known as the C.I.A triangle. According to Mattord and Whitman (2012), the concept of C.I.A triangle was originally developed by the computer security industry and it has been used since the development of the mainframe. In a way, the C.I.A triangle deepens the understanding of protecting information because it tells the critical characteristics of information that should be protected. In fact, information security is usually described as the protection of information by preserving confidentiality, integrity and availability. (ISO/IEC 27000, 2014; Mattord & Whitman, 2012; Nist glossary, 2013). Since confidentiality, integrity and availability are mentioned so

often in infosec literature, in the next subchapter these key concepts and few others are explained in more detail.

2.1.1 C.I.A - triangle and other key concepts of information security

Confidentiality of information - In short, confidentiality of information means that only those with permission should be able to see a particular piece of information. Information has confidentiality when it is protected from disclosure. Confidentiality ensures that the access to information is possible only for those with assigned rights. So then if someone without the proper rights has access to the protected information, confidentiality is breached. (Mattord & Whitman, 2012.)

Like infosec in general, confidentiality is related to both business and non-business environments. In organizations confidentiality can be breached by simple carelessness of not disposing important documents in a proper way. More importantly, organizations often hold important personal information that should remain confidential. Individuals who transact with an organization expect that their personal information will remain confidential. In this way, confidentiality and privacy are closely linked. (Mattord & Whitman, 2012.)

Integrity of information - Information has integrity when it is whole, complete and uncorrupted (Mattord & Whitman, 2012). Integrity in information security means that sensitive data should not be modified or deleted in an unauthorized or undetected manner (Nist glossary, 2013). In plain English, integrity here means that the users of information should be able to trust that the information they use is genuine and in its authentic state. No one without permission should be able to delete or modify important data. On top of that, measures for preventing corruptness (caused by viruses or noise in transmission media etc.) should be in place.

Availability of information - "Availability enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format." (Mattord & Whitman, 2012, 12). An information system should always be providing information when needed and when this is not happening the availability is obstructed and security is breached. In an organization, system failure is one type of information security issue (Backhouse & Dhillon, 2000). Of course system failure is a security issue for home users as well, even if measures for prevention might not be as big in magnitude as with organizations. Another example of availability in infosec is to prevent denial of service attacks, since these attacks cause loss of availability for users (Aura, Leiwo & Nikander, 2000).

Authenticity of information - According to the latest ISO/IEC standard authenticity is defined as "property that an entity is what it is claims to be." (ISO/IEC 27000, 2014, 2). Another definition describes authenticity as confidence in the fact that a message, transmission or message originator is valid (Nist glossary, 2013). Confidence comes when something is verifiable and trusted. In this way authentication is closely related to authenticity. Authentication

establishes confidence of authenticity by verifying identity of a user, process or a device (Nist glossary, 2013).

Non-repudiation - Non-repudiation, which can be defined as the "ability to prove the occurrence of a claimed event or action and its originating entities." (ISO/IEC 27000, 2014, 7), means that a sender of a message is not able to deny the sending of the message afterwards and the recipient cannot deny ever receiving the same message. In addition to being able to prove message delivery and reception, non-repudiation can mean a capability to determine whether an individual performed an action such as creation and approvement of information (Nist glossary, 2013).

Accountability - "Accountability, also known as auditability, ensures that all actions on system—authorized or unauthorized—can be attributed to an authenticated identity. Accountability is most often accomplished by means of system logs and database journals, and the auditing of these records." (Mattord & Whitman, 2012, 250). In infosec accountability is a security goal where actions of individuals or entities can be traced uniquely to that individual or entity. This in turn helps for example in fault detections, intrusion detection and legal action. (Nist glossary, 2013.)

So then, based on the above, what can be concluded about the meaning of information security? Surprisingly, national institute of standards (Nist glossary, 2013) puts it all together quite nicely and defines what information security is:

> Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
>
> 1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
>
> 2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
>
> 3) availability, which means ensuring timely and reliable access to and use of information. (Nist glossary, 2013, 95.)

But is this everything one needs to know about information security then? Some say that the traditional C.I.A does not fully capture the meaning of information security.

2.1.2 Expanded C.I.A and risk management

The traditional view of information security, based on the C.I.A triangle has being challenged in different sources (Anderson, 2003; Mattord & Whitman, 2012). While this is true, it must be said that the triangle itself is not questioned. The question is, does it capture the meaning of infosec completely. Is infosec all about the protection of confidentiality, integrity and availability of information? A very conservative approach to this problem is to simply expand the triangle

with new concepts, some which have already being discussed in the previous subchapter (non-repudiation, accountability, authenticity). Mattord and Whitman (2012) say that the protection of C.I.A is as important as it has ever been but it no longer adequately addresses the constantly changing environment. For this reason they introduce an expanded model consisting a list of critical characteristics of information. The list consists of confidentiality, integrity, availability, accuracy, authenticity, utility and possession.

A slightly different approach to explaining information security stems from the term risk. To put it simply, information has value to an organization (or individual), therefore if information is jeopardized, business (or individual) suffers. In this way there are information risks that should be managed. Blakely, Geer and Mcdermott define information security as "risk management discipline, whose job is to manage the cost of information risk to the business." (Blakely et al., 2001, 2). In another source it is mentioned that information security minimizes the risk of exposing information to unauthorized parties (Venter & Eloff, 2003). As already mentioned, this approach of risks and risk management does not conflict with the earlier definitions of protecting information by preserving the C.I.A. Instead it describes more of the process of information security. A definition of information security (organizational context) from Anderson (2003) is a good way to understand how information security is always a process of finding a balance between information risks and their countermeasures: information security is "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, 2003, 310.) According to the author, being *well informed* means there is expertise in both the area of information security and the particular business environment. No two organizations are alike and every organization has its own needs and characteristics, including unique information security requirements. *Feeling assured* is achieved when there is clear knowing that the data, in which the whole information security program is based on, is reliable. *Information risks* are catalogued in specific manner for the specific enterprise and then *controls* are assigned to each one of them in order to reduce risks and increase assurance. But for information security to work, it must be in *balance*. A delicate process of balancing costs and threats that answers to question: How secure can we afford to be — or need to be?

As conclusion, adding the term risk to the equation of defining infosec furthers understanding of the concept. Risks are always probabilities that something might or might not happen. It is good to be aware of different risks but also of the likelihood of something bad happening. Only this way proper, cost effective countermeasures can be assigned.

2.2 Information security behavior defined

This short subchapter focuses on explaining what is information security behavior (IS security behavior) in the home use context. It seems there is no clear or

generally accepted definition of IS behavior at home setting. For this reason the subchapter mainly narrows the topic down to clarify what is meant by home IS behavior in this thesis. Clarification will help the reader in knowing better about the topic of the study.

Home user IS behavior is a difficult thing to describe. First of all as mentioned before, there seems to be no clear, generally accepted definition of home IS behavior in the scientific literature. Second, IS behavior is a very vast and complex area which hardens the task of defining it. One could consider updating firewall, not opening e-mails from unknown sources or setting of complex passwords as types IS behavior. Basically the list could go on forever so clearly there is a need for better approach.

A useful way of explaining home user IS behavior in a simple way is to talk about precautions that need to be taken in order to secure ones information, devices etc.. Home users might be a risk to themselves or others in the internet and for this reason it is essential that users recognize risks and take appropriate precautions towards security (Li & Siponen, 2011). Similarly, Agarwal and Anderson (2010), who studied the factors influencing home user IS behavior, narrows their research objective to: understanding individuals willingness to take recommended security precautions under individuals own control to protect themselves and the internet in general. These precautions are defined as "individual actions such as running and consistently updating antivirus software, utilizing a firewall, being suspicious of e-mails from unknown sources, and effectively securing passwords." (Agarwal & Anderson, 2010, 614.)

Concluding from all this, IS behavior of home users in this thesis means: taking on recommended security precautions to ensure the safety of own computers, laptops, smartphones, other internet devices and the internet as a whole. Recommended security precautions are generally accepted information security measures that one can find or hear about in different medias which aim to improve people's information security as a whole. To address the research questions more thoroughly, home user IS behavior is extended to mean the omission of known security measures and precautions. After all, it is also interesting to know why some people knowingly neglect information security measures when they operate in the World Wide Web.

3 EXPLAINING INFORMATION SECURITY BEHAVIOR - ORGANIZATIONS

Information security behavior of employees in organizations has received quite a lot of attention from researchers. Possibly one of the reasons for this is that employees have difficulties in following organizational rules and guidelines regarding information security (Ifinedo, 2012). For example, when it comes to organizational information security policies (i.e. rules, requirements and guidelines relating to safe use of information systems), it's not enough that the employees are aware of such guidelines and rules. Employees need to comply with the policies as well. But as said, it seems this is not happening in organizations and for this reason, getting information on how to encourage employee compliance is one area of interest to researchers. (Siponen & Vance, 2013.)

This chapter takes a look at the relevant literature of employee information security behavior. This review is not a complete depiction of the research field. Rather, aim here is to give an overview of different research streams and relevant theories that are used in explaining employee information security behavior. As said, this thesis is mainly interested in explaining home user information behavior. Nevertheless, chapter contributes to the overall understanding of individual's information security behavior, whether in workplace or home. In addition, there are similarities in theories and factors that explain both home use and workplace behavior.

The chapter is divided into two research streams: "**computer abuse/misuse**" and "**employees information system security policy compliance/noncompliance**". Even though these two streams are separated, they are not mutually exclusive and there is a clear overlap between the two streams. For example, using unauthorized systems is both a violation of most information security policies but also an example of computer abuse. The division is more artificial, meaning that most of the articles in the review have been divided to either of the chapters, solely based on the title of the papers.

3.1 Computer abuse/misuse

According to Siponen and Vance (2013), the term computer abuse can be traced as early as the year 1976 when the term was first introduced by Donn B. Parker. Computer abuse has been defined as the unauthorized and deliberate misuse of information systems (Straub, 1990; Harrington, 1996). Violations can be done against hardware, software, data and computer services (Straub, 1990).

A common theory applied in computer abuse research is the deterrence theory (Warkentin & Willison, 2013). Deterrence theory (DT) has been used in studies such as (Straub 1990; Harrington 1996; D'Arcy, Galletta & Hovav, 2009). In fact deterrence theory is widely used in IS security research as a whole (not just computer abuse) and particularly in behavioral IS security studies (D'Arcy & Herath, 2011). The theory is rooted in criminology and suggests that there can be disincentives that deter a person from committing a crime. If the risk of being caught is high and the penalties from committing a crime are severe, deterrence theory posits that individual will not commit a crime (Siponen & Vance, 2010). Theory is based on the rational choice view of human behavior: illicit behavior can be controlled by the threat of sanctions that are certain, severe and swift (D'Arcy & Herath, 2011). In the theory two sub constructs are usually used, "certainty of sanctions" and "severity of sanctions". In computer abuse research these two sub constructs are used to examine whether deterrence theory can predict employee behavior. For example, if the employee knows that he is going to be fired (certainty and severity of sanction) if he is caught of unauthorized modification of data, it can be hypothesized that the employee is not going to continue with this course of action unless he is sure he won't get caught.

Earliest article in this literature review, that uses deterrence theory in order to explain computer abuse, dates back to Straub's research of "effective IS security - an empirical study" in 1990. Study was successful in applying DT to explain the behavior of employees. According to Straub (1990), IS security deterrents (such as increased IS security efforts) result in reduced incidence of computer abuse. Organizations that clearly state their policies against computer abuse and actively enforce these policies benefit from less abuse. Key is to inform the staff about proper system use and about the penalties that may result from non-compliance. Another study (Nance & Straub, 1990) suggests organizations should give increased attention to detection activities towards computer abuse as well as punishing perpetrators to fit the crime. Also, serious abuse incidents should be reported to authorities more often. According to the study, these suggested guidelines should work as deterrents to the employees.

Harrington (1996) investigated if codes of ethics can deter unethical behavior in computer abuse context. Employee judgments and intentions were studied. In the case of computer abuse, codes of ethics had no significant effect. General codes of ethics in organizations had no effect while IS specific codes of ethics had a small effect in the intentions and judgments of employees on com-

puter abuse. Although the codes of ethics had little effect, they shouldn't be discarded completely, says the author. Instead, codes of ethics can work if there are other useful tactics in place as well.

In more recent studies in computer abuse, DT has not been the only explaining theory. In fact, new theoretical frameworks have been created using different theories and DT together. Also, it has been said that deterrence is not enough to explain this abusive behavior. For example, Dinev, Hu, Ling and Xu (2011) discovered that deterrence alone is not going to be effective in reducing employee information security policy abuse. The study used rational choice as its core and other theoretical frameworks as periphery to form a new model to explain information security behavior. Model hypothesized that individual behavior depends on the rational calculus of costs and benefits. This cost benefit evaluation is affected by three forces: individual propensity (degree of self control), individual moral beliefs (judgment of right and wrong) and perceived deterrence. Individual propensity and moral beliefs were found to shape individuals behavior more than deterrence. In practice, the study suggests screening for employees that have high moral standards and self control.

There are other studies that have mixed deterrence theory with other theories or extended the existing DT to better explain computer abuse/misuse behavior. D'Arcy et al. (2009) integrated user awareness of security countermeasures, sanction perceptions (DT) and IS misuse intentions into one model called extended general deterrence theory. The results suggested that user awareness of security policies, SETA (security education, training and awareness) programs, and computer monitoring each have some deterrent effect on IS misuse intention. Also perceived severity of sanctions was found to be more effective than certainty of sanctions in deterring misuse. Finally, impact of sanction perceptions were found to vary based on individuals level of morality. Basically this means that moral commitment and IS misuse intentions have highly significant relationship between each other.

Lee, Lee & Yoo (2004) used DT and social control theory to better explain human side of computer abuse, which according to the authors, was lacking in research at the time of the study. In short, the article brought a new factor, "organizational trust", into the research field of computer abuse. Organizational trust is shown as the individual's commitment, attachment and involvement to the organization (and fellow employees) as well as individuals view on norms. It was found that the enhancement of social bonds through organizational trust could help in preventing computer abuse in organizations. Deterrence on the other hand was not a significant factor in reducing computer abuse.

All in all, computer abuse has received considerable attention in IS security field (Siponen & Vance, 2013). Findings from studies using deterrence theory have been found inconsistent, sometimes contradictory and inconclusive (D'Arcy et al., 2009; D'Arcy & Herath, 2011). Similarly, cases in this subchapter have already shed some light on deterrence theory, computer abuse and of the results, which have been found to be inconsistent at times. The point here is not to declare that deterrence theory has no explanatory power at all. It does ex-

plain some of the behavior but the theory has not been conclusive. For example Dinev et al., (2011) point out that while deterrence can explain some of the behavior of employees, it often cannot explain everything.

Maybe one of the main points of this subchapter is to understand what is deterrence theory since it has such a big role in behavioral IS security research. As DT is used in different streams of behavioral IS security research it's worthwhile to explain a little of the field and the differences. Warkentin and Willison (2013) introduced a continuum of information security policy violations, where violations are classified based on the employees intent. Employee intent can be intentional and malicious computer abuse, volitional but not malicious noncompliance or passive non-volitional noncompliance. This subchapter of computer abuse would situate somewhere between "intentional malicious computer abuse" and "volitional (but not malicious) noncompliance". For example D'Arcy et al. (2009) mentions IS misuse domain to usually vary between unethical and inappropriate behavior (e.g. personal use of company e-mail) and illegal behavior, such as accessing confidential company information. According to Warkentin and Willison (2013), most of the studies concerning information security policy compliance/noncompliance have focused on well intentioned employees and examined factors which either hinder or facilitate compliance with security policies. These studies would then situate in the middle of the continuum as "volitional but not malicious noncompliance". From this knowledge, it's easier to continue the literature review on subchapter about employee information security policy compliance and noncompliance.

3.2 Employees information security policy compliance and noncompliance

Information security policy (ISP) research usually focuses in understanding, how employee compliance could be achieved in regards to these policies. In these security policies: organizational rules, guidelines and requirements are laid out to influence employee behavior with respect to how organizational IS resources are used (Ifinedo, 2012). An ISP prescribes how organization manages, protects, and distributes information (Nist glossary, 2013). Unfortunately it has been suggested that employees don't readily comply with such documents and guidelines (Ifinedo, 2012; Benbasat, Bulgurcu & Cavusoglu, 2010). For this reason Ifinedo (2012) highlights the importance of studies explaining the issues that inhibit or encourage the compliance of ISP among employees.

In this subchapter such studies are reviewed to give a picture of what factors shape employee information security behavior in regards to security policies. But first, to better understand what kind of behavior is usually investigated in these kinds of studies, a list of typical IS security violations are presented here. This should give a more practical view on what kind of issues are happen-

ing in organizations. Siponen and Vance (2010) reported the most common and important IS security violations in organizations to be:

- Failing to lock or log out of workstations,
- writing down personal passwords in visible places,
- sharing passwords with colleagues or friends,
- copying sensitive data to insecure USB practices,
- revealing confidential information to outsiders,
- disabling security configurations,
- using laptops carelessly outside of the company,
- sending confidential information unencrypted and
- creating easy-to-guess passwords.

3.2.1 Protection motivation theory research

One of the very common theories applied in ISP compliance research has been protection motivation theory (PMT). The theory has been found to be one of the most powerful explanatory theories, predicting individual intentions to take protective actions (Agarwal & Anderson, 2010). Although the theory has roots in social psychology and health domain (Ifinedo, 2012), it has been noted that PMT has been used successfully in over 30 areas such as politics and environmental protection (Mahmood, Pahnila & Siponen, 2010).

PMT measures individuals coping behavior when he or she has been informed of a threatening event (Rippetoe & Rogers, 1987). Individual will then try to cope with the threatening situation and the response (to threat) is determined by two cognitive processes, "threat appraisal" and "coping appraisal". Threat appraisal consists of components called "perceived vulnerability", "perceived severity" and "rewards". These components will tell to the individual, how likely is it that the threatening event will occur, how severe would the consequences be and what are the rewards for not adopting a recommended coping response. It should be noted that this process is individuals own subjective assessment of the situation. As an example from an article (Low, Tan & Woon, 2005), a threatening situation could be that a smoker hears cigarette smoking is linked to lung cancer. Here a person will evaluate how vulnerable he is to lung cancer, how severe would it be to get lung cancer and what rewards (eg. psychological pleasure, peer approval) he can get if he continues smoking.

Coping appraisal on the other hand consists of "self efficacy", "response efficacy" and "response costs". These components will tell how well the person can cope with and avert the potential loss or damage resulting from the danger. Continuing with the smoking example, self efficacy refers to the individuals confidence in the ability to quit smoking, response efficacy refers to the potential health benefits of quitting smoking and response cost refers to the withdrawal symptoms that the smoker might suffer. (Low et al., 2005.) In ISP compliance then, suggested by PMT, employees are seen to assess:

- can they save work time (i.e. rewards) by not complying with policy,
- how vulnerable they are, if they don't follow security guidelines (perceived vulnerability),
- what happens if the threats are realized (perceived severity),
- do they have the necessary IT skills to comply with the guidelines (self efficacy),
- will compliance with ISP actually result in increased security (response efficacy) and
- will compliance with ISP cause inconvenience to actual work (response cost).

Based on these constructs, behavior will then follow to either compliance or noncompliance of ISP.

PMT research in ISP compliance is usually combined with other theories. Ifinedo (2012) created a model applying theory of planned behavior (TPB) and a reduced PMT to explain employee intentions towards ISSP (information system security policy) compliance. Both of the theories have self efficacy as a common construct but TPB added two new construct to the existing theory of PMT: "subjective norm" and "attitude towards ISSP compliance". Subjective norm in the study hypothesized that if fellow peers, subordinates etc. follow ISSP: s, the employee will most likely abide with the guidelines as well. It was also hypothesized that positive beliefs and values (attitude) about the ISSP will have a positive effect on employee compliance. It was empirically validated (survey of 124 employees) that attitude towards ISSP, subjective norms, self efficacy, response efficacy and perceived vulnerability, all positively influence employees intentions to comply with policies. Hypotheses relating to perceived severity and response costs were not supported.

In another study (Pahnila, Siponen & Vance, 2012) PMT was integrated with habit theory. Interestingly an empirical test showed that habitual IS security compliance strongly reinforced the cognitive processes theorized by PMT, as well as employee intention for future compliance. In addition, most of the results from the empirical research were consistent with PMT assumptions. Perceived vulnerability had an insignificant impact on employees' intention to comply with IS security policies which was a surprising result. This would indicate that the respondents did not feel that policy violations could subject them to security threats. Study also investigated if rewards (component of PMT left out from many studies) affected intentions and it was shown that if not following a security procedure can save time on actual work, employee probably won't follow the procedure. Finally, results highlighted the importance of addressing employees' past and automatic behavior (i.e. habit) in order to improve compliance.

Herath and Rao (2009) used a model applying PMT, deterrence theory and TPB to develop a framework explaining employee compliance. Similar to earlier results such as (Ifinedo, 2012; Lee et al., 2004), organizational commitment and

social influence (subjective norms included) had significant impact on compliance intentions. Another important discovery in the study was the relationship between computer self efficacy and resource availability. Employees provided with such help as computer training and online availability of the security policies are better equipped to comply with policies hence enhancing intentions towards compliance. In regards to DT, results were again mixed. While certainty of detection had an impact on employees, severity of penalties did not. PMT in the study was linked to employee attitudes towards policies, not intentions. While PMT components affected the attitudes of employees, there was no significant link between attitude and intentions to comply with security policies. Nevertheless a post-hoc analysis revealed that self- and response efficacy had direct influence on compliance intentions. Threat appraisal and response cost on the other hand had no impact on intentions. Finally, authors found that employees in the study sample seem to underestimate the probability of security breaches. (Herath & Rao, 2009.)

Many of the earlier results were also supported by Mahmood, Siponen and Pahnila (2007). In the article, habits and normative beliefs were found to affect employee compliance intentions significantly. Partly in line with Herath and Rao (2009), sanctions derived from deterrence theory had no impact on intentions. Easy and quick access to policy documents (information quality) was found to have a direct effect on actual compliance behavior as well, while facilitating conditions positively impacted attitudes of the employees towards complying with information security policies. In regards to PMT constructs, coping appraisal had no impact on employee attitudes towards complying with security policies. Threat appraisal on the other hand did. (Mahmood et al., 2007).

As a conclusion on protection motivation theory research in ISP compliance, the theory seems to predict employee intentions and behavior quite well, which has also been mentioned by Ifinedo (2012). But, as the examples in the subchapter reveal, PMT alone is not enough. There are many other theories and explanations to employee IS security behavior and ISP compliance, a view which has been noted by Agarwal and Anderson (2010) as well. All of the previously mentioned research focused on general policy compliance behavior but PMT has also been applied to specific threats such as spyware. Theoretical model strongly influenced by PMT, was able to explain the adoption of anti-spyware software in a university setting (Johnston and Warkentin, 2010). This would indicate that PMT is indeed quite powerful in explaining security behavior in many ways. Although PMT is useful in this research stream, it should be noted that certain research results might be affected by the study subjects, i.e. whether IT experts or non experts are studied. It was discovered that, in the adoption of anti-malware software in small and medium sized enterprises, IT experts were more affected by threat appraisal and social influence while the non experts were more influenced by coping appraisal and IT budget (Larsen & Lee, 2009).

3.2.2 Other ISSP compliance research

While the previous articles all had PMT as a common factor, they are not that different from many other studies in the ISP compliance research. Benbasat et al. (2010) used rational choice theory and TPB to form their model on ISP compliance. Again normative beliefs (perceived social pressure caused by behavioral expectations of colleagues, executives etc.) and self efficacy were found to influence intentions to comply with policies. Big focus in the article was to find out how attitude towards complying is shaped and whether this attitude also influences intentions to comply with security policies. Employee attitude towards compliance was found to influence intentions and the attitudes themselves are shaped by beliefs such as **benefit of compliance** (expected favorable consequences), **cost of compliance** (unfavorable consequences of compliance e.g. work impediment) and **cost of noncompliance** (unfavorable consequences of noncompliance). Information security awareness was also found to have a positive influence on overall compliance of employees.

Rational choice theory was also applied in article studying the compliance of internet use policies. Internet abuse can be defined as all kinds of non-work related internet activities such as checking personal e-mail etc.. Employee intentions were found to be influenced by cost benefit analysis, personal norms and organizational context factors. Cost and benefit analysis evaluates risks such as security risks and penalties sanctioned from misuse of internet, against benefits such as convenience and more interesting work life. If costs are perceived to be small then misuse behavior will probably continue but this evaluation process is also affected by personal norms. Strong moral sense of individual is less influenced by the cost benefit analysis. Personal norms can further be influenced by organizational context factors which refer to organizational norms. (Li, Sarathy & Zhang, 2010.) Finally, authors mention that, organizational norms can eventually become a part of employee's internal norms.

Compliance has also been researched from viewpoints such as mandatoriness. Employee noncompliance with ISP: s has to be explained, at least partially, by the employee perception that following security policies is not mandatory. Otherwise it should be expected that more employees would comply with security guidelines. Boss et al. (2009) introduce the concept of "mandatoriness" which refers to the perception that complying with security policies and procedures is compulsory and expected from the organizational management. Acts of specifying policies and evaluating behavior were found to be effective in convincing that security policies are mandatory. Mandatoriness itself was found to be effective in motivating individuals, as the authors put it: "if individuals believe that management watches, they will comply. "(Boss et al, 2009, 151.)

3.3 Summary of key factors explaining employee information security behavior

Overall there are many theories and explanations for behavior of employees, some which have not been even discussed in this chapter. For example it has been suggested that national culture differences might also play a role in explaining information security behavior (D'Arcy & Hovav, 2012). It is also noteworthy to recognize different types of information security behavior of employees suggested by Warkentin and Willison (2013). Sharing a password to fellow employee with good intentions probably won't be explained by same factors as deliberate destruction of organizational data.

Although different theories and models deepen our understanding of the phenomenon, certain general reasons can be highlighted to explain employee information security behavior. Summarizing from previous subchapters, poor or forbidden behavior can be affected by measures such as:

- Issuing severe and certain sanctions and enhancing the monitoring activities to better detect misuse of information assets,
- providing training, awareness and resources to employees so that they are better equipped to comply with policies and guidelines,
- improving organizational trust and employee commitment overall and
- convincing employees that compliance of ISP is mandatory.

Some overall factors affecting employee behavior found in the previous chapter are:

- Individual moral beliefs,
- social influence and subjective norms,
- self efficacy i.e. skills and confidence that provides employees the ability to comply with the organizations information security policies
- employees assessment of threats (threat appraisal) i.e. perceived severity and vulnerability of threats and
- habits.

4 EXPLAINING INFORMATION SECURITY BEHAVIOR - HOME USER

Although there are many studies explaining information security behavior in the workplace, they might be less relevant for the home user research. For example, home users IT activities are not monitored nor are there mandatory training required from them, information security wise. (Agarwal & Anderson, 2010.) While there might be similarities between organizational use and home use, differences need to be recognized in order for research and practice on home context to develop further (Li & Siponen, 2011). Certain contextual factors have been theorized to point out how information security might be different under different contexts. For this reason, factors explaining employee behavior, which were outlined in the end of last chapter, are not completely applicable in home use and a separate research stream is therefore needed. To sum up the key points, home user behavior might be different from workplace behavior because:

- home users hardly ever receive awareness training nor is there evidence that workplace training would transfer into increased home security,
- there is no IT support, home users need to use their own expertise to secure their PCs including the safeguarding of the network with software and hardware,
- there is no monitoring of/ sanctions for poor behavior,
- safety climate towards information security might be hard to form at home because it relies on the effort of all the family members,
- protection procedures are not mandatory at home and
- home devices might have several users increasing the difficulty of managing computer security. (Li & Siponen, 2011.)

The most obvious differences from the factors that explain employee behavior are related to sanctions, monitoring activities and the expected mandatory compliance towards rules that don't exist in the home context. Deterrence theory and the relevant studies in computer abuse therefore have little to contribute in home context. Nevertheless, the following chapter shows how there are simi-

larities and organizational studies can therefore contribute to home user research as well.

This chapter takes a deeper look into the research field of home user information security behavior. One of the significant result in the literature review is the lack of research conducted in the field. Eleven articles were selected for the chapter and they were mostly chosen based on repeating citations cross referenced in other papers. One of the papers (Li & Siponen, 2011) takes a look on home user research and concludes that more research is needed. They also theorize main differences from workplace context to clarify how home user research could be further developed. As such the article has motivated much of the current thesis. Two of the articles (Bryant et al., 2007; Gritzalis et al. 2013) were chosen to paint a better picture of what kind of information security behavior is being reported based on surveys and to point out there are shortcomings when it comes to safe computing of home users . Latter of the articles discusses the secure use of smartphones which is still a very new topic in the field of information security and behavior research. In improving the situation of home user information security one of the papers (Herley, 2009) takes another viewpoint on the subject and claims user neglect on information security is entirely rational. This is based on an economic perspective meaning that usually the burden of security is far greater than the benefits from acting in secure ways.

The more theoretical articles were found to consist some familiar concepts and theories such as coping- and threat appraisal and protection motivation theory (Agarwal & Anderson, 2010; Low et al, 2005; Enbody, Larose & Rifon, 2008; Herath et al., 2014; Liang & Xue, 2010) as well as theory of planned behavior (Ng & Rahim, 2005; Lee & Kozar, 2008). Some of the studies also focused on particular protection procedures such as e-mail authentication, spyware adoption and protection of wireless network.

4.1 Theoretical research and explanations on home user behavior

This chapter begins with a summary of one article. As said, research in the field of home user information security behavior is scarce at the moment. Still, Agarwal and Anderson (2010) conducted a thorough research on the subject and for this reason it is the basis for this theoretical chapter that discusses different factors influencing home user information security behavior. Later, results from Agarwal and Anderson (2010) are discussed in relation to other research on the field. Many of reviewed literature have a lot of things in common with the mentioned article.

4.1.1 Agarwal and Anderson (2010) - Practicing safe computing

Research into safe computing of home users was divided into two separate studies. The first one focused in understanding drivers of intentions to perform

security related behavior and the second one in the interventions (marketing messages) that can positively influence these drivers. What was different in the study was that individual's intention to perform security related behavior was split into two components intention to protect one's own computer and intention to protect the internet. There is a clear difference since the first component has only personal consequences but the latter has wider impacts (e.g. spreading virus to others). Based upon the protection motivation theory, the first study revealed that self efficacy, response efficacy and concern regarding security threats all had an impact on the individuals attitude to protect both own computer and the internet. (Agarwal & Anderson, 2010.)

In addition, a concept of psychological ownership was introduced into the research model. Psychological ownership tells how much an individual feels ownership to an object and the more the individual feels ownership, the higher is his desire to protect the object. Increased investment of time and energy to one's computer (computer customization etc.) is assumed to increase the individual's sense of ownership. Likewise, using more activities that require the internet will increase the sense of ownership to the internet. It was empirically validated in the study that the level of psychological ownership does in fact influence the security related behavior in securing both own computer and the internet as a whole. (Agarwal & Anderson, 2010.)

Finally the effects of norms (subjective and descriptive) were found to influence behavioral intentions. Opinions of important others and normative beliefs i.e. subjective norms were found to influence intention to secure own computer but not the internet. This could be explained by the fact that individuals can lose more if they do not protect their own computer. Also, individuals might believe that, it is their role to protect their own computer while protecting the internet on the other hand is a jointly held responsibility. The belief of what others are doing to address security (descriptive norm) was found to influence intentions to protect the internet but not own computer. (Agarwal & Anderson, 2010.)

In the second study an experiment tested how messaging (marketing messages) could influence attitudes and intentions towards security related behavior. While most of the authors' hypotheses regarding the experiment were not supported, some important findings were reported. First both subjective and descriptive norms can be influenced with message cues. Second, messages focusing on positive outcomes vs. negative outcomes were found to be more persuasive in promoting safe online behavior. (Agarwal & Anderson, 2010.)

4.1.2 Threat and coping appraisal i.e. protection motivation theory

Many of the results that Agarwal and Anderson (2010) found have been discussed and validated in other research articles. A study focusing in wireless networks at home (Low et al, 2005) validated most of the components of PMT. Study attempted to explain how the decision to implement security features on home users wireless networks is influenced. In addition to self efficacy; per-

ceived severity, response cost and response efficacy were all found to be significant factors in explaining why users implement or don't implement security features. Further support for PMT came from Liang and Xue (2010) as they highlighted the importance of both coping appraisal and threat appraisal (i.e. PMT) to explain IT threat avoidance behavior. In the context of adopting anti-spyware software, authors summarized:

> This paper conveys a simple, yet powerful message – to motivate computer users to avoid IT threats, they need to be convinced that the threats exist and are avoidable. If users fail to see a threat, they will not act to avoid it. If they see the threat but believe it is unavoidable, they will not act to avoid it, either. Thus, both the threat appraisal and the coping appraisal are necessary to motivate security behaviors. (Liang & Xue, 2010, 403.)

4.1.3 Self efficacy

Self efficacy is a construct found both in protection motivation theory and theory of planned behavior. For example, in two studies regardless of different theories (TPB vs. PMT), both definitions of self efficacy seems to be in line with each other. First, in a PMT influenced research, Agarwal and Anderson (2010) defined it as: "The individual's belief in his/her own ability to take the recommended precautions" (Agarwal & Anderson, 2010, 623) while an article related to TPB defined it as: "home computer user's self-confidence in his/her skills or ability in practicing computer security" (Ng & Rahim, 2005, 239). Reason why self efficacy is so important is that, it's not only about the skills; it is also about the confidence to tackle new challenging situations. Self efficacy has been noted to be perhaps the most powerful educational strategy safety wise. (Enbody et al., 2008.) Seven of the reviewed articles mentioned in this chapter all talked about the self efficacy and mostly (one differing impact) it was validated as an important factor influencing home user security behavior. In all of the articles it had an impact.

First, Agarwal and Anderson (2010) conducted a more general research meaning that no specific protective measure was selected, to survey sample subjects. Self efficacy was found to positively influence attitudes towards security related behavior and attitude was significantly linked to behavioral intentions to secure one's own computer. Two of the studies found that in the adoption of anti spyware software, self efficacy plays a big role (Lee & Kozar, 2008; Liang & Xue, 2010). In the case of protecting one's own wireless network, Low et al. (2005) discovered that those who possess higher knowledge tend to secure their networks on their own when compared to those with less knowledge. One of the studies combined three protective activities: updating anti-virus regularly, backing up of critical data and using firewall and suggested the necessity of equipping home computer users with the necessary skills to use technical solutions (Ng & Rahim, 2005). Finally, self efficacy was found to influence positively to intentions (towards safe online behavior) in a controlled experiment of 206 students (Enbody et al., 2008). In the adoption of e-mail authentication service,

results were interesting. Self efficacy was found to negatively influence the intention of using such a service. Overall, the article suggested that those with higher self efficacy might engage in risk taking behaviors. It was suggested that higher self efficacy results in higher confidence in the individuals abilities hence making the service more pointless compared to those who are not that confident in screening e-mail themselves. (Herath et al., 2014.) Nevertheless, judging from the articles mentioned, it´s quite safe to predict that high self efficacy overall will also result in better information security among home users.

4.1.4 Subjective norms

One of the repeating themes in this literature review of home user security behavior has been subjective norm. To clarify the meaning of the concept, Ng and Rahim (2005) define subjective norm as: "This refers to a person's perception of the social pressure to perform or not to perform the behavior under consideration, in this case, to practice computer security in home computers". (Ng & Rahim, 2005, 238.) Determinants of subjective norms in the relevant studies, to name a few, have been family and peer influence, mass media, visibility and image. Enbody et al. (2008) briefly states that if we believe that our spouses and co-workers wish that we would be safer online, then this belief will have an influence on us. Further evidence of peer and family influence can be found from Ng and Rahims (2005) article. Peer influence was found to weigh more than family influence but all in all, authors suggest we should always remind those around us of the importance of securing our computers. Also mass media as a channel for education in the security context should be fully utilized as it was found to have a crucial role in promoting computer security. Finally, an important viewpoint to subjective norms was that if people perceive adoption (of technology like safety measures) as an opportunity to enhance their image as an ethical/moral and technical leader among their referent, they feel more social pressure to adopt (the technology) (Lee & Kozar, 2008). This finding was found in the context of adopting anti-spyware software.

4.1.5 Attitude

Attitude, as previously mentioned in this thesis has been found to have a direct impact on intentions to engage in secure behavior. Like in the case of subjective norms, different determinants have been found to influence attitudes of home users. Perceived usefulness in the case of adopting anti-spyware software was found to have a significant influence on attitude (Ng & Rahim, 2005). This means that if users think performing a particular practice will enhance their security, they will see it as useful. Therefore usefulness of computer security practices should be stressed to users (Ng & Rahim, 2005). Attitude can also be influenced through relative advantage and compatibility which can be summarized as:

> In the context of anti-spyware software adoption, people develop a positive attitude toward adopting anti-spyware software when they perceive it as an effective tool to enhance security and privacy of their systems. In addition, the more the adoption of anti spyware software fits an individual's needs, values, and other protective methods, the more favorable the attitude he/she can develop toward anti-spyware software. (Lee & Kozar, 2008, 112.)

Agarwal and Anderson (2010) also found attitude to influence intentions but their determinants were derived from PMT. As already mentioned self efficacy, threat appraisal and response efficacy all impacted the attitudes of home users toward security related behavior.

4.2 Surveys on home users – reported behavior

While the theoretical research explains information security behavior of home users quite well it is also beneficial to take a look at some more practical research on the subject. Theoretical models explain the factors influencing user information security behavior but it is also beneficial to know what exactly are the users doing wrong or right and how they report it.

Survey of 415 home users to assess perceptions of security issues and attitudes towards the use of related safeguards was conducted by Bryant, Furnell and Phippen (2007). Survey revealed that while users claimed confidence in their abilities on information security matters, deeper inspection contradicted this premise. For example, while many respondents answered they know what common security threats (virus, spyware, hacker etc.) mean, a portion of the subjects did not choose to take any relevant safety measures against these threats. When it came to updating these malware-related software's the results were even more daunting. Only 37% confirmed updating firewall regularly and the highest result (updating anti-virus regularly) got only 63%. Authors pointed out though that some of the updating is done automatically these days, so the figures might not be as bad as the survey suggested.

Another important finding in the survey was related to the skills of the respondents and the results gave further evidence of self efficacy being important factor in home user security behavior. IT novices, as the article named them, seemed to agree it is their responsibility to protect their own devices but they lacked the confidence and skills to do it. Majority of the issues were knowledge based meaning that users did not know how to protect themselves and they were not aware of initiatives that could help them. Interestingly, advanced users seemed to be vulnerable as well even though they claimed to be confident in protecting their systems. All in all, the article suggests that there is shallow knowledge among home users in security related topics and this knowledge needs to be developed deeper with education and awareness. This is a job for official and mass media: To go beyond simple definitions and shallow knowledge to a more effective learning foundation. (Bryant et al., 2007.)

In the context of smartphone usage and security awareness, not much research has been conducted (Gritzalis, Kastania & Mylonas, 2013). Considering the rise in the number of smartphones that connect to services that use the internet, the volume of research might increase in the near future. Gritzalis et al. (2013) focused on studying how smartphone users deal with security when downloading software from official application repositories. It is suggested that attackers can use this centralized application delivery architecture to advantage. Survey was answered by 458 smartphone users. First, the results revealed that 76% of the sample population trusts the official application repositories such as google play or windows marketplace. According to the authors it is unclear where this sense of trust comes from because the majority of respondents were also unaware if there is any application testing mechanism in these repositories. Second, smartphone users tend to ignore security messages that are prompted to them and some ignore all the messages that the application might display, further weakening their smartphone security. Third, once more self efficacy was found to be a key factor since those who answered to be security or technically savvy seemed to pay more attention to security messages. Also, those that had their smartphone security controls disabled were found to be the technically less skilled individuals. Fourth, majority of the users did not have any third party security software installed in their smartphones and of these respondents, most reported using security software in their personal computers. This would indicate that users don't see threats in a similar way when they use smartphones to connect to the internet. Finally, authors conclude that the trust in official repositories is a severe security vulnerability. (Gritzalis et al., 2013.)

Both of the selected articles paint a sad picture when it comes to information security of home users. While only two surveys were discussed, it has been mentioned in many sources, such as (Agarwal & Anderson, 2010; Li & Siponen, 2011; Ng & Rahim, 2005), that when it comes to information security, the home users are the weak spot and a threat to both themselves and the internet. Reasons for why this is the case have been discussed in this chapter. Overall, home computer users intention to perform security-related behavior is influenced by a combination of cognitive, social, and psychological components (Agarwal & Anderson, 2010).

Situation naturally raises questions: How can the situation be improved and who should try to improve it? One additional reason for the bad situation might be explained by the simple fact that education of home users on information security topics has failed, as Herley (2009) puts it:

> Users, we have seen, are not irrational: exhaustive lists that seek to avoid all potential harms are not helpful to them and are ignored. If we want a different outcome we must present a better tradeoff. How did we manage to get things so wrong? In speaking of worst-case rather than average harm we have enormously exaggerated the value of advice. In evaluating advice solely on benefit we have implicitly valued user time and effort at zero. (Herley, 2009, 143.)

4.3 Call for more research

The literature review started out from organizational context to explain employee information security behavior. Different factors were found from various articles that explain employee behavior. In addition, part of these factors were found to explain home use as well. For example both employees and home users go through a process of threat appraisal and coping appraisal and certain behavior follows. In both research streams, especially self efficacy was found to be a big factor in the coping appraisal process of individuals. Finally, in home context more factors explaining home user behavior were found.

As the two surveys from the previous subchapter revealed, home users are showing behavior that puts themselves in risk and this has been acknowledged in more theoretical papers as well. There is a need for research and clearly the discussed articles have contributed to this area of interest. While a big problem is that there is not much research done in home context, there are also some challenges in current research that this thesis tries to remedy.

Articles about home use that were discussed in this chapter are mostly quantitative where sample sizes have been in hundreds. Such sample sizes naturally bring constraints on the research. Much of the current papers have focused in specific countermeasures such as protecting wireless home networks or adopting spyware software. For example, Liang and Xue (2010) mention choosing spyware as the malicious IT threat but acknowledge that their results might be different if the threat changes. Further, the purpose in their study has been purely in empirical testing. But as Li and Siponen (2011) mention the limitation in such studies is that they merely tests if existing theories are supported or not. Li and Siponen further suggest inductive qualitative research with theory development in mind. Such approach could produce new constructs, concepts and even theories to why home users behave in certain manner.

So in short, it can be concluded that while much research in organizational context has been made it does not fully explain information security behavior of home users. Research in home use has also being conducted and factors to explain user behavior have been discovered. Nevertheless, much of research has being quantitative in nature and there is need for qualitative approaches as well. For these reasons, the empirical part of this thesis is conducted with a handful of interviews to see if something new to the phenomenon of information security behavior could be found. No existing theories are used; instead the study starts from clean table with theory development in mind. Such research is not bound to any specific safety measures and the interviewees have more room to explain why they show certain type of behavior (good or bad) in information security. In addition, if some type of conflicts occur in interviews (e.g. interviewee reports he/she is not using anti-virus software) it can be further discussed to find out why this is the case and this way there is a possibility to get much more detailed information on home user behavior.

5 EMPIRICAL RESEARCH - RESEARCH SETTING AND METHODS

This section explains more about the empirical part of the research that was conducted during the year of 2014. Main research questions are first listed and explained in short manner. After that the actual research setting is described to clarify how answers to the research questions were attempted to be discovered and why selected research methods were chosen.

5.1 Research questions

Main research questions are the following:

- What are the factors that influence home users information security behavior?
- Why users adopt some of the safety precautions while dismissing others?

First of all it is interesting to know the factors that influence home user information security behavior. Knowing the factors can help in improving the situation among home users that use the internet on a daily basis. Some users on the other hand have adopted numerous safety measures. It is interesting to find out how this happens. What is the story behind it? Likewise users, even those that adopt some safety measures, can dismiss other measures. It is equally interesting to know why this type of situation occurs.

5.2 Selected research methods

In getting to know more about the relevant literature on home user information security behavior it became clear that the empirical part of the study should be

done using semi structured interviews and the research should focus more on theory development rather than testing the existing frameworks. As mentioned earlier in the thesis, there is limited understanding to what influences home user behavior (Agarwal & Anderson, 2010). In such situations where understanding is limited, it has been suggested that using research methods like grounded theory is a good way to approach the issue (Puusniekka & Saaranen-Kauppinen, 2006). Decision was made to use grounded theory (GT) as a framework for implementing the study by highlighting theory development. Such research methods (GT and theory development) have also been suggested in literature for home user context (Li & Siponen, 2011).

In grounded theory the idea is to discover theory from analyzing the data. Dey (2004) describes GT as a way of generating theory through research data instead of testing ideas that have been formulated in advance. Dey suggests that GT relies on acquiring qualitative data through variety of methods such as unstructured interviews in the initial stages of the research. In the analyzing phase the data is coded into categories. These categories are conceptualizations of the key aspects of the data. Successful conclusion to research is achieved when theoretical saturation is achieved. At this point the new data is not refining or improving the theory. After the research has reached saturation the researcher can develop a story that encapsulates the main themes of the study. (Dey, 2004.)

The actual interviews were based on the idea of semi structured or focused interviews. In such interviews there are no predefined detailed questions that are expressed to all the participants. Instead, there are certain themes around the research topic that are discussed with the interviewees. These themes have been planned beforehand but no specific questions are used. The actual interview situation resembles more like a normal conversation where room for open discussion is given. The interviewer can also ask follow up questions when needed. (Puusniekka & Saaranen-Kauppinen, 2006.)

5.3 Research process in this thesis

Using the ideas from GT and focused interviews, the research was conducted in a specific manner and the theory development was iterative in nature. In the beginning, interviews were quite loose and different themes were tested to see how participants responded to different questions and what topics brought up the most discussion relevant to the study. As the interview process developed, certain themes started to repeat in discussions. Repeating themes were named (or coded) and at that point all of the conducted interviews so far, were listened again to see if the coded themes occurred somewhere else. For example, after a while it became evident that bad experiences influenced home users. At that point the interviews were listened again to see where bad experiences were mentioned and what the interviewees said about the topic.

When going through the interviews it became obvious that many of the participants were talking about the same themes in various contexts. Each occurrence of a coded theme was written on a notepad. Every note had a description of what the interviewee had said. Notes were further coded to either *good or *bad to indicate whether note explained good or bad information security behavior. As an example, below is one example of one line from the notes. The theme belongs to bad experiences, there is description of what had happened and the line also indicates whether the experience influenced the interviewee in a positive or negative way: "**bad experiences (lost control of e-mail account due to phishing scam) *good**."

Once all of the interviews had been done (saturation was reached after 13th interview), the notes on each topic were combined to a designated text file. Every note was listened once more and the most important phrases were also transliterated from the recorded audio. The interviews were done in Finnish so the transliterations had to be translated as well for this thesis.

When all of the repeating themes had been separated to their own text-files (including the transliterated content), the actual analysis of the content was done to make sense of the story and the related themes that had been discussed throughout the interviews. This is when the actual writing of the next chapter happened.

5.4 Research setting

Overall (13) subjects took part of the research and the interviews were recorded using recording software of a smartphone. Interviews lasted from 25 minutes to 45 minutes. Subjects had no common demographic factor. Ages varied between 24 and 58 and the only common factor among subjects was that they all use computers and internet at home on a regular basis. Most subjects also used smartphones.

Questions were divided into different interview themes relating to safe internet and computer use. Selected themes were derived from chapter 2.2 where common information security behavior is described. Themes, although not all of them, were the following:

- Adoption and use of security software such as anti-virus and software firewall,
- e-mail security,
- password principles and use,
- backing up of private and valuable data,
- internet banking procedures and
- laptop, tablet and smartphone security.

The interview themes themselves were not that important. Instead the research setting was planned to inspire discussion about these topics and draw

interesting comments and phrases from the subjects as the interview went along. As an example, most information security guides highlight the importance of having complex passwords. They also highlight that one should change them regularly and one should not have same passwords to different services they use on the internet. So then, when discussing the forming of passwords with the interviewee, either "good" or "bad" behavior would come up. This is the area where the research was interested in. What is story behind subject's willingness to take the effort to form solid passwords? On the other hand why someone would make easy passwords willingly? In a similar pattern different themes were discussed and fortunately most of these discussions brought up results to the actual research questions. Actual analytical inspection to the research data and resulting conclusions are discussed in the coming chapters.

6 ANALYSIS

The following chapter consists of the actual analysis part of the interview data that was collected during the year of 2014. The research process was already described in the previous chapter. As said, interviews were done in Finnish. The most important examples were transliterated and also translated into English. Interviewee comments were used in the text of this chapter to better illustrate how certain conclusions were drawn. It was important to translate every interviewee comment as close to the original phrase as possible but some compromises had to be made for grammar considerations. Yet all of the comments represent what was actually said during the interviews. Interviewee comments are highlighted with cursive markings *("like the text in here with quote/unquote marks in the beginning and the end")* to make the text more understandable to the reader.

Actual content of the chapter consists of the broad themes or conceptualizations that arose in the interviews. As mentioned before, focus of the empirical part of the study was in theory development where key aspects of the interviews are encapsulated to discover theory from the research data itself. Overall five distinct themes arose and repeated in the interviews enough to form claims about how home users information security behavior is influenced. Further implications of the analysis are then discussed in the next chapter.

6.1 Forced and automatic safety measures

"Forced and automatic safety measures"- theme means: measures that the users cannot control themselves and that the measures are automatic in nature i.e. they take care of themselves. From the user point of view this means, for example that a user cannot form easy to guess password, instead a service demands the user to make a more difficult password. Another example is when operating system takes care of important updates automatically without the user even noticing. In addition, the theme has been extended to mean such situations

where the activation of certain safety measures has been done somewhere else and the user receives these measures "automatically". Such situations are common for example, when certain security related software are installed to computers before they are sold by vendors. Finally, some examples in the analysis are situations where automation should be in place but for some reason it is not there. Forced and automatic safety measures were discussed in most of the interview themes such as: security software use and adoption, password forming principles and use, e-mail security, laptop security and smartphones.
It is not a new idea to have automatic safety measures. Yet in the interviews the nature of the theme started to form certain interesting "stories" that revealed a lot about home users. First of all, in worst cases the whole information security of a user might be at the hands of automatic safety measures. Second, it would seem, based on the data from interviews that even the skilled users neglect safety occasionally if it's not forced upon them. The following chapter reveals how the theme arose to discussion in interviews.

The unskilled user: "*Yes I have something (security software), it came with the laptop, I think it came with the laptop…I can't really name it for sure, maybe it's Avira*". Here, a user who admits to be less skilled in information security matters describes how she initially secured her own laptop with antivirus software. User continues that she wouldn't even know how to procure or install these kinds of security software on her own. Yet, while the information security matters seemed overwhelming, many important safety measures are in place. When asking about the habits of updating security software, same interviewee responded: "*Yes (I update), because my laptop suggests I should update, that's when I do it.*" On another subject she continued, "*When I got it (laptop), the computer suggested me to secure it with username and password*." While the user saw real value in securing her laptop with a password it was clear that the automatic nature was the main reason for causing the interviewee to adopt this particular security measure. In general, it seems that the subject here benefits from having things done automatically. This is a classic example of automatic safety measures but other interesting subject arose in the interviews as well.

When automation fails..: One interesting case involved a skilled user whose operating system refuses to update itself due to some software related errors. The user reports he has always taken care of security updates, especially windows updates, as according to the interviewee, they are automatic and therefore easy to manage. User explains: "*Lately windows has started to imply my operating system might not be a genuine version, even though it is, and I haven't bothered to register it to Microsoft via internet. So from the point of view of Microsoft, my operating system is not genuine and the updates are not working anymore...I should probably take care of it because my windows updates are not up to date anymore...it has lasted for few months...I think this is one of those projects that never gets done, I know I should fix it but I never do.*" Interviewees reasons for the situation lasting so long is that, he doesn't really see risk in the current situation but if it changes, then he will fix the update problem. The challenge with this logic is that it relies on the fact that somehow the service provider would inform the user about a serious vulnerability before any attackers recognize the same thing. If the situation

is vice versa, user will be seriously vulnerable until information about the threat reaches him. The example implies an important message, when automation fails, information security measures might be neglected and "poor" behavior patterns might develop, even among more skilled uses.

Suggested but not forced measures: In the context of changing passwords regularly, two cases similar to last example highlighted the importance of having automatic and forced safety measures. When giving the choice to the user, information security might be neglected, which in turn partly explains poor information security behavior of home users. This is what one of interviewees had to say: *"I had one service that automatically forced me to change password (occasionally). It seemed like a good idea".* But when changing of passwords becomes voluntary, the same interviewee explained: *"sometimes I have changed passwords on my own but quite rarely. Problem is that I have 20 passwords and if I would change them all it would take a lot of effort."* A striking case of risky behavior arose in the context of internet banking and password protection, further validating the importance of forced safety measures instead of voluntary: "M*y internet bank actually notifies me from time to time that this would be a good time to change a password and it's wise to change them regularly. But it doesn't actually force me to do it and to this day I still have not changed my password. Kind of weird when I say it out loud since it's my bank and money we are talking about."*

When measures are forced and not just suggested: Quite the opposite happened when one of the users explained how he ended up (or was forced to) securing his laptop by having his username and password requested every time someone wanted to use the computer. *"In my laptop I have a picture where you need to press three dots in the right place in right order to unlock...I have it because in windows 8, when you login, it's mandatory to ask for a password...it came with the package when I bought it, it was forced on me...I haven't bothered to find out if I could disable the feature...if it had not been forced on me I probably wouldn't have it enabled."* It would seem that when automatic and forced safety measures are not easily disabled it might lead to higher information security.

Two devices, different approaches: Similarly and interestingly to last example, one of the interviewee reported that his iPad was secured with lock screen password but his smartphone wasn't. This is not the same feature as pincode that is requested when you turn a device on. This safety mechanism is such that when already powered on, after not using the device for a while, it goes into a mode where you have to confirm identity with a password to resume using the device. This is often referred as "lock screen". Interviewee elaborated: "*Actually you cannot use my iPad if I forget it somewhere but you CAN use my smartphone...it's a good question (why this has happened), in iPad it was there from beginning. As long as I've had smartphones, and this is my third, it has not come up anywhere that I could enable such feature that it would ask for password...now that I really think about it, it would make most sense to secure my phone since it's the easiest to misplace...After this interview I will probably check if I can enable it but this is one of those situations where it might be difficult to find the actual moment where I would have the energy and time to actually secure my phone*". It became obvious that the idea of securing iPad or smartphone made sense to the user yet iPad was the

only thing secured because of forced lock screen. Another interviewee had a similar situation with his smartphone. It then turned out that the phone was from the same manufacturer as the previous example. Subject confirmed he checked if it is possible to enable such feature but he couldn't find it from the phones settings. After that he didn't bother to look for a separate app. This then lead to lessened information security on his phone. Manufacturer differences might explain some differences in smartphone security. But most importantly, yet again, giving the choice to the user proved to be a lessening factor when it comes to information security overall.

All in all, in automatic safety measures, easiness and practicality was highlighted and it is also related to better information security. Automation can be the first line of defense when getting a new computer, for example when the user has not installed anything themselves. Some interviewees mentioned how e-mail sorts out the junk mail better these days so the user don't have to deal with it themselves. But also it should be noted that forced measures don't necessary mean higher information security. Many of the interviewees confirmed they use same passwords to different services and mainly because of practicality concerns. Here the password might be safe (because of forced mechanisms) but information security slightly decreases as the same password is used over and over again. Yet the most important part in the interviews was related to how users react when automation fails or measures are not forced. It would seem that in these types of situations information security decreases. Therefore choice should not be on the user when important information is at stake and disabling safety measures should be made difficult.

6.2 Bad experiences

Bad experiences – theme, by its name is quite self explanatory. Almost all of the interviewees at some point of their lives had experienced something really bad when using the internet. Interviewees really wanted to share these experiences and it was encouraged. At times, participants felt that information security as a topic is something difficult; there is a lot of technical "jargon". But when they started talking about bad experiences the stories came out quite naturally. While interesting these stories might be, in terms of the research questions it is also important to understand how these experiences have influenced the users. Or have they? Based on the research data, most of the bad experiences were positive in a sense that they ultimately lead to heightened information security. Bad experiences arose in all of the interview themes from virus infections to backing up of private data.

Hands on experience: One of the interviewees is a relatively skilled computer user. In addition, on regular basis, he helps his less skilled computer using friends and relatives with information security problems, e.g. installing right kind of software or cleaning viruses from computers. This is what he had to say: "*I remember installing some older windows version in the past, as it had in-*

stalled enough so that I could connect to the internet the computer was already infected just because I didn't install antivirus immediately... So I am worried that if there is no security software in place in computer, there is definitely threat in the internet…also I have friends and all sort of relatives who have had viruses in computer. As I had to clean these systems it has indeed occurred to me that it is beneficial to have some programs in place"

The threat really exists: The good thing about negative experiences is that the idea of information security threats transforms from something abstract to something real. Similar to last example, when asked if one of the interviewees sees a real threat in the internet he replied *"Well yeah, there was this trouble in my workplace, happened when our virus protection wasn't proper, the workplace pc transformed into a junk mail server. In the end the service provider had to disable the whole internet account (because of the traffic in generated). After that information security (in the workplace) was updated but yes it has influenced (taught) me as well."*

Not learning from bad experience: The important part about learning from these experiences is that one needs to know where things went wrong and what one could have done differently. This was not the case in one of the examples where one of the interviewees was so compromised the easiest thing was to reinstall the whole operating system. This is what he had to say: "*did I learn anything? I have to say probably not, which sounds stupid but I honestly don't know where the virus came from. I had not done anything different than I have in the past 10 years; suddenly I have this virus that locks my screen".*

Unable to prevent bad experience: Another interesting case was one where a user couldn't have prevented information security breach. According to the interviewee, some time ago "Playstation 3" accounts were hacked and a lot of personal information, including credit card numbers was stolen. Subject says it's possible his information was compromised too. The event has made the interviewee reluctant to give credit card information to the internet. If he has to do it, it's to a provider that is someone he knows and is trustworthy. The decision is smart and a good example of how information security behavior is not just installing security software to a computer. It is a process where the user needs to make judgment calls regularly about how to conduct in the internet. This point is especially proved in the next example where one interviewee described how he lost the control of his own e-mail and instant messenger account. What made the case interesting was that it happened to a relatively skilled user.

Bad judgment: Interviewee was advertised about a program that could tell if some of his instant messenger contacts are blocking him. This means that the user cannot see any of the "blocking" contacts online or communicate with them. "*I googled if it's possible to find out who has blocked you in messenger, and then I visited this site that asked me to enter username and password and it will be shown who has blocked you*." Unfortunately the interviewee gave the asked login information. The site showed some shady data and the interviewee was convinced quite fast that the information is made up. Not so long after, this happened "*my contact friends in messenger were saying to me that "you are sending some weird messages, what are they?" … They were advertise type of links asking my friends to visit certain sites…At that point I realized my account had been "abducted"…I did eventu-*

ally get control of the e-mail… Yes, (I learned that) you should not give your login information anywhere." The harsh reality is that even skilled users can be exposed to information security threats with one bad judgment and this was not the only case where perpetrators where able to phish out login information from a skilled user. In the next example a user was scammed with a carefully executed ploy.

Carefully planned ploy: One subject was a victim of losing account login information due to carefully planned ploy. The case happened partly due to bad luck and the mistake done by the user was not big: *"There is one discussion forum account that was stolen from me…I noticed it was out of my hands when my password was changed and I couldn't log in…The same thing happened to a lot of people…Some hacker had made an exact copy of the discussion forum, a faulty wrong site that was so well implemented it was identical to the original, just like they try to do in internet banking these days when they send those fake e-mails phishing for passwords…why I had bad luck was that I didn't have the original link to the website so I had to Google it and via Google I got the fake site. So there I logged in and the hacker got my login information…(After the incident), if my money or identity information is at stake, I learned to be cautious, I look at things(in the internet) completely differently and if something seems out of the ordinary I'm very careful."* Situational awareness was something the subject had learned from the experience which is important when judgment calls need to be made.

Emotional experiences: One particular subject that was discussed a lot in the interviews was the backing up of pictures that had been piling up over the years and the related negative even sad experiences, when these photos had been lost. "*I have once lost all my photos…it influenced me, I don't want to lose them anymore. Important phases in my life were lost and those photos are nowhere anymore…one mishap needed to happen before I decided to do something about it.*" Sometimes it's enough to see others having bad experiences for learning to occur as one interviewee put it: "*So many friends relatives etc. they have lost files. I have seen it so many times, pictures have vanished and you cannot get them back. I don't want that to happen to me*".

Overall, there were a lot of shared experiences that arose in the interviews, some that have not being mentioned here. For example one interviewee explained how her virtual goods got stolen in a virtual hotel, where users can purchase furniture and decorate their own place. In one case user decided to activate the lock screen on his phone after he had lost it momentarily. But as mentioned, in terms of the research question it is important to know if bad experiences improve information security and how? Mostly it seems that information security increases from bad experiences if users know what they did wrong and know how to prevent it from happening in the future. Bad experiences are especially good because the feeling of threat is then very real, not just something that you hear from news etc. that does not concern you. This way, countermeasures to threats are seen as something important too. But it is not given that bad experiences lead to heightened information security or that learning would occur every time something bad happens. In the mentioned case where virtual goods ended up stolen, the subject only replied that she

doesn't use that kind of game services anymore. Here the response was quite passive. Another interviewee had his phone infected with some kind of malware when using a wireless network in an airport in Greece but he thought it was a special case and he is still quite willing to use public networks whenever he needs connection to the internet.

6.3 External influence

External influence as a theme means influence that is coming from outside and has an effect on users information security behavior. Mostly this means news and warnings in various medias about viruses and other threats as well as advices from friends and other peers. Based on the interviews, external influence seems to be an important factor in the original adoption of information security when knowledge has not yet been accumulated by the users. It has also, at least partially, influenced experienced users to re-evaluate their security in the internet due to increase in warnings. A common "story" mentioned in the interviews was related to time period when internet became much more popular, connections got faster, old dial-up connections were updated to broadband ones. Here news and warnings played a big role but it is important to mention that since these things had happened many years ago, related stories were a bit vague. One interviewee tried to remember the original adoption of security software: *"During the time when windows 98 was the popular operating system it became obvious viruses are a real problem, I probably stumbled on it while reading a popular computer magazine at the time, I can't really say for sure, if not the magazine, there were lot of news, because during those times viruses were really spreading and it was recommended to use firewall and antivirus.* When asked if the interviewee thought the original adoption of security software was due to external influences he affirmed this by reasoning that he did not learn anything at home from parents, so the adoption intention must have come from external source.

Advices from a mix of sources: Sometimes the external influence can come from more than one source and a mix of these advices or warnings might end up in the adoption of security software: "*Originally it started when I bought (his first) computer and began to use the internet. Gradually I installed some programs, mostly free ones. This is because I constantly got messages from the internet, prompting me to keep my security up to date and there were constant virus warnings. Also, in school, when I was still studying, the topic strongly emerged as an issue".*

Peer support: One of the participants told a story where a relative was insisting he should install antivirus program to the interviewee's computer. Even though the interviewee was reluctant, the situation seemed to have a permanent effect: "*The first time I adopted (antivirus software) was when one relative was visiting us, I still lived at home. The relative started to talk about all kinds of information security issues, kind of showing off how he knows about these things, and eventually he installed antivirus to our computer…I thought to myself that he might as well install the program since he seemed to be fixated on the matter. I didn't really adopt the*

use of antivirus programs at that point but ever since I've always had some security programs on my computer"

Media influenced paranoia: One particular example was an interesting case of how external influence can almost cause the opposite behavior than intended: "*Everyone talks about it everywhere (about information security), and there are all these ads in the internet saying that if you don't use those programs you get some damn virus and your whole computer is messed up. It's been talked about so much that you get this sense of paranoia in case you don't have those (security) software. That's the only reason I use those programs. But today I thought, well I got this suspicious feeling that would you even get any viruses (without the programs)?* Later the interviewee specified that maybe this increase in all kinds of warnings is just a way to sell information security software to average users. Nevertheless, in the end he confirmed he cannot really afford to not use software. He doesn't want to take any risks.

When it comes to **internet banking**, different medias seemed to have done a good job on alerting people on possible threats. In the interviews this was mostly reported as more cautious behavior on the internet. When discussing the warnings related to internet banking here are a few examples of what came up in the interviews: *"I have tried to make sure I only use internet bank on my own computer. I don't use it on open networks and if I'm planning to use it on my friends computers I always check that they have all the protection enabled."*

"*Especially when I'm taking care of banking stuff or something else very important, I'm more cautious and careful than before because lately there have been a lot of email scams and attempts and if I'm giving my credit card number on the internet I'm going to check twice where my card info is going*".

"*I wouldn't use it (internet bank) on internet explorer because I've heard there have been a lot of information security vulnerabilities on that browser*".

Last case related to internet banking was when one interviewee, not so skilled in the information security matters, explained she had read about a phishing scam, where people had lost money. Apparently, the scammers had made a fake site that looked very real and many people had thought it's the real thing. Fooled by the fake site, people ended up giving their login information to the scammers. *"It's a bit horrifying that something like that is possible. When I use my internet bank services I really make sure it's the right one."* Clearly the news seemed to be a bit shocking and revealing to the interviewee. Seems she did not even know these kinds of scams are possible.

External influence due to the interview process: One of the interviewees actually enabled his lock screen on his phone due the interview process. This is the same person (discussed in the previous chapter of forced and automatic measures) who had the screen lock activated on his iPad but not on his smartphone. As it turned out, situation was caused by the simple fact that the feature wasn't an automatic on his phone. When discussing the matter, the interviewee realized that out of all of his devices, his phone is most likely to get lost, so it would make the most sense to secure the content of the phone with the lock screen. After this revelation, the interviewee said he would probably enable the screen lock after the interview. Few months after, when checking if

this had actually happened the interviewee responded on sms message:"*I had not found the time to do it earlier but I enabled it one minute ago. It helps if someone who knows about these things reminds me yet doesn't pressure me to do something. If no one reminds me though, I probably forget about it completely.*"

Overall it seemed that if the phone didn't suggest lock screen automatically, advices from friends and other peers influenced the interviewees in a positive way, like in these cases:

"*My brother asked me if I have a lock screen on my phone. He recommended that I should consider it because my phone is always on the internet and I have many accounts like e-mail linked to the phone. It did sound very reasonable so I enabled it.*"

"*Some of my friends said you should get this lock screen, you can draw your own pattern that opens the phone and no one else can access it, and since it was easy to enable I decided to get it*".

All in all, interviewees were able to specify instances where external influence has played a role in improving their information security behavior. Unfortunately a lot of the stories were a bit vague, it can't be concluded how these external factors influence users. There is clearly an increase in the awareness of threats, acquired through different medias. But does heightened awareness and sense of threats lead to better information security behavior? One interviewee said he is more aware of different threats but he doesn't think it influences his actual behavior. On the other hand, some examples directly showed that external influence affects users, like the cases where users enabled their smartphone screen locks due to suggestions coming from outside. Lastly, it would be interesting to know that when an interviewee says he or she is more cautious because of the hype in media, is there actual improvement in information security behavior occurring.

6.4 Value of information

Value of information as a theme means that users seem to value their information and based on the evaluation they either are interested in protecting their information or not. Indeed, it would seem based on the interviews that a big factor in explaining poor information security behavior is the evaluation process people go through when deciding whether something is worth protecting. Value of information as a theme repeated a lot in the interviews but mostly in the context of passwords. In plain terms, the theme suggests that while credit card information is something to value, account to a local restaurants information system is not.

People engage in poor behavior willingly and knowingly, because they don't see the value of doing it differently. For example one of the interviewees phrased it like this: "*I'm very lazy, I never update or change my passwords. I've had the same passwords for many years now. If it's something important like university account I make them more complex. But for example if it's some account to my local barber shop I really don't care what the password is or if someone gets it*".

It would seem that most people in the interviews know it's against common recommendations to keep same passwords to different sites or that it's unwise not to change passwords regularly. But according to the interview data, in most cases the effort to secure an account in some public service is not worth it. Users don't want to practice conscientious computing. As one of the interviewee put it: "*I have two so called trash passwords that I can use for example in certain gaming services. My world won't come crumbling down if someone would be able to hack these types of accounts... I use the same password in these kinds of services because it makes my life easier. Valuable accounts like facebook or e-mail where I have personal information, I have different passwords…It's mostly because of my laziness that I don't want to put effort to secure these useless services*".

The two quotes in the previous paragraphs repeated in almost every interview in different forms. Some users might have been a bit more conscientious in using different passwords to different accounts, but when it came to changing passwords on a regular basis no one thought that it would be worth the effort unless the information is really important. One of the interviewees mentioned something noteworthy. The interviewee explained he has at least 20 different accounts; forming a new password to each and every one of them and then changing them regularly seems utterly ridiculous. This is something that is difficult to argue against.

The subject of information value was discussed in backing up procedures as well yet there was nothing interesting to report. For home users the idea of backing up information is a bit tricky in a sense that you can't force the users to back up something nor is there any reason for it. It's the users own private data and it's completely up to them whether to back up or not. The only one who potentially loses information is the home user himself. This is one big difference to organizational settings. It's also understandable that people back up important valuable information and ignore the unworthy. One could argue that this is the basic idea of backups.

Overall, interviewees seem to value their information and depending on the evaluation, security behavior results. Limitation in the chapter was that it was mostly discussed in the context of passwords. Indirectly it has been discussed in other areas as well. In the last chapters, the often mentioned "careful and cautious behavior" is definitely linked to situations where the user sees something of value to be at risk, for example in the context of internet banking. Or in choosing whether to secure smartphone with lock screen or not, there were examples where the interviewees realized they definitely had something valuable inside their phones and protecting the content with lock screen is a good idea.

It is worrying though that the interviewees willingly practice unsafe behavior in the internet at times. Such practices might lead to risking others as well as mentioned in the introduction. Security behavior means also securing the internet as a whole. When mentioning this to some of the interviewees they usually replied that they had never thought about it, yet agreeing it is something to consider. This would lead to conclusion that if people knew more about this they might act differently, in a more conscientious way.

6.5 Skills, awareness and information security

Skills, awareness and information security as a theme explains how information security is either practiced of neglected based on the readiness of the user to practice safe computing. Unlike in previous themes, the content didn't always come up in straightforward way. There was a lot of reading between the lines or trying to get the feeling whether the interviewee feels comfortable in a given interview topic or not. This was the case with skilled and aware users. Most of the less skilled users were honest in their responses and it was clear when some kind of poor security behavior is occurring in the interviewee's life. One interesting feature in the "skills of the interviewees", is that a lot of the skilled users think what they do is just common sense. Sometimes it was even difficult for them to elaborate how they have adopted certain patterns of behavior etc. that keep their computers secure.

Lack of knowledge - "I don't know", "I have never heard about that kind of thing", "I can't": Interviews with the less skilled participants were quite different in nature when compared to the interviews with the more skilled users. There were a lot of negatively formed phrases like "I don't know", "I can't" or "I have never heard about that". One of the basic routines one can practice to keep computer safe is to scan for viruses. This is what one of the less skilled interviewees elaborated on the subject when asked if she regularly scans for viruses: "*I don't know how to do it, never. It has not even occurred to me. I have never heard of "scanning of viruses"*. When the interviewer clarifies it means searching of viruses from one's computer the same interviewee continues*: "No, I don't know how to use it. I would probably ask my brother to do it."*

Same kind of "lack of knowledge" was present in other instances. When asked if information security in general feels difficult or it takes too much effort interviewee replied: "*Yeah, usually I need to ask others about it (help in information security). The only thing I have heard is that you should have a virus program. If it gets more complicated I'm going to need help."* Another example arose when discussing operating systems security updates: "*I can't really use my laptop to anything else but browsing the internet, I don't know how to take care of it (security wise)."*

Skills or awareness?: A question that arises when analyzing the content is that, do people neglect information security because they are simply unaware of certain guidelines or is following the guidelines too difficult for them. There were direct examples and more general thoughts in the interviews that might suggest that a big part of the neglect is simply due to lack of awareness. One of the discussed topics in the interviews was related to using the internet outside of home, whether it's via public wireless networks or public and shared computer stations one can find in libraries etc. One of the basic guidelines in public unknown networks is to practice caution and to avoid using services that demand login information, for example using facebook or e-mail. One of the interviewees put it shortly: "*If I have to access my email I access it anywhere, I never thought it could be harmful…I have never thought that it's risky.*" Lack of awareness was also apparent when interviewee explained why she doesn't consider risks

when using wireless networks in public places: "*If I get free wifi then good. The only thing I consider is that the guy who didn't block his wifi has been careless. I've always thought its just access to internet. How can it be risky?*"

In a more general level same type of answers came up when the interviewees were asked, how they feel about information security in general and what kind of thoughts the interview process have possibly brought up. "*Stuff we have discussed here for example, I think I would have welcomed this kind of information earlier. I'm not familiar with these kinds of issues even though I use internet every day, you don't really think about the risks.*" One of the interviewees thought she could be able to learn how to practice better information security, her "poor" behavior was more about the "not knowing": "*I think I could learn if I had heard more... that "you should do like this" etc., I don't think it would be that hard.*" Whether it's due to lack in awareness or skills, risky situations occur if users are not careful. The same interviewee from last phrase described her habits of downloading movies from peer to peer - torrent networks: "*Sometimes I download movies from the internet because a while ago I learned how to do that. At times it's a bit of a gamble what (file) I'm going to choose… I'm not aware of a way where you could check beforehand if the file is malicious*." There are indeed ways to check the authenticity of these types of files, mostly via peer comments. Usually fake or malicious files are "flagged" so that people could stay away from harmful data. Legal matters aside, peer to peer networks are a breathing ground to many questionable materials and user cautiousness is important.

Confident and informed: When discussing information security matters, quite fast the interviewer developed a sense that the subject clearly knows what he or she is doing. Then, it no longer was a question of how skills explain information security behavior. It was more about, how skills and awareness comes up in the discussion, when talking about these matters. For example, when discussing why someone would use protective software, one interviewee put it like this: *When I'm out of my comfort zone, shady sites etc., you easily get something (malicious) to your computer.(With security software) at least your computer has a back up if you accidently click on banners... Or if you have guests over who are not that skilled in computer use, it's good to have some back up so you don't find your computer messed up the next day."*

Information security related skills show up in many ways in the interviews. In one instance one of the interviewees explained how spyware and malware works and why it's good to use software that encounters these threats. There were also few cases where the interviewees explained they like to read reviews and evaluate different security software rather than installing any random program that comes up. In the case of e-mail use, almost all of the interviewees elaborated how they usually neglect and delete suspicious messages; they don't open attachments, they discard junk mail in order to keep their accounts safe. One of the skilled users elaborated how he forms passwords and why: "*Usually in my password I have at least seven characters with one big letter and a number…I don't use generally known words in my passwords. Some programs can try to guess passwords and if you have big letters or numbers it's much more difficult. I haven't really read about this, somehow I just have received this information from*

someone." Clearly skills show up in these phrases and it seems to lead to better information security behavior. Yet it might be difficult to track, where this knowledge originally came from. Common sense was an often mentioned word among the more skilled interviewees: *"Well, you need to use common sense too, if you're browsing shady web sites you don't click "ok" to everything you stumble on. At that point your software can't help you since it's you who gave the permission for installation (of malware etc.)"*.

In conclusion, various IT related skills and developed awareness about information security threats plays a role in explaining safe computing in the internet. Nevertheless, there have been cases in the interviews where compromises in safety happen even though the risks are known for the skilled users. For example overconfidence might develop as two of the skilled users reported they don't protect their smartphones with a separate lock screen. This was justified by explaining that they are not going to lose their phones. Another justification to the matter was that writing a pin code every time you take the phone out of your pocket is too much effort. Furthermore, in relation to previous chapter of information value, password security is not given enough effort if the service is considered to be less important. What feels important in the current theme is the gap between those who are skilled and those who are not. In the interviews there were many cases where these two groups intertwine. It seems family, friends and other peers might give help and support to those who need it. An interesting question is how these support links could improve so that the knowledge could be transferred more efficiently. Not just when one's computer is already hijacked and the user is denied from his own device.

7 DISCUSSION

The interviews set out to find factors that influence home users information security behavior. Fortunately such factors emerged in the discussions with the participants. Based on the interviews, some claims of how information security behavior is either positively or negatively influenced can be formed. As such, the study was successful in finding answers to the initial research questions of what factors influence home user information security behavior and how information security behavior is either positively or negatively influenced i.e. why safety measures are adopted or dismissed by the users.

Information security behavior is positively influenced by forcing automatic safety features to users. In the case of less skilled users, automatic and forced measures can help in adopting challenging safety measures. More experienced users on the other hand tend to neglect information security at times if the measures are suggested but not forced. Therefore, if possible, the safety features should not be voluntary and disabling them should not be too easy. All in all, users seem to like the easiness and practicality of these automatic features. The idea of improving information security by forcing measures is not new in the workplace environment. Automation and mandatory security measures is in fact a known subject in the workplace settings where it has been proposed by the IS community that the "knowing doing" gap of employees could be fixed by promoting such measures. "Knowing doing" gap refers to a situation where people know how to protect their systems but fail to do so and apparently such behavior is occurring in organizations. (Bommer et al., 2008.) Also, Li and Siponen (2011) mention that in organizational context, security has a feature of compulsoriness since the decision of adoption of security software is made by the organization and not the employees. In fact such compulsoriness is mentioned as one of the key aspects that differentiate home use from organizational context. Considering the implications from the interviews, such compulsory and forced measures are important in the home user case as well if overall security should be improved. While automation is often available to the home users, it seems to be up to them whether to activate this helpful tool.

Bad experiences related to information security positively influence user behavior. If the user knows what went wrong when bad experience happened, it would seem some learning occurs that leads to better information security. Bad experiences give the user a real sense of threat that is out there on the internet. It's not something theoretical anymore, something that does not concern you, but a real threat that can cause anything from mild discomfort to monetary losses. It should be noted though that not all mentioned bad experiences in the interviews have lead to better information security behavior. In relation to the existing literature, bad experiences are something old and new at the same time. For example, Bommer et al., (2008) mention that people who have been victimized in the past (in information security) can see themselves as victims again. What is new is that there seems to be linkage between threat appraisal and bad experiences. So far (to the knowledge of the author) such linkage has not been discussed in the context of information security behavior. Threat appraisal has been confirmed as a significant factor in promoting safe computing (Agarwal & Anderson, 2010; Liang & Xue, 2010; Low et al., 2005). Therefore, according to the interviews and the existing literature it could be theorized that bad experiences influence the threat appraisal process of individuals and as such contribute positively to the overall information security behavior of individuals.

Home user information security behavior can be influenced with external forces. In the interviews such forces were warnings and news in the various media about threats in the internet as well as family and peer influence. Media influence is strong in the original adoption decision when the user has not adopted certain safety measure yet. Warnings have also caused some more skilled users to re-evaluate their security by having an increased sense of threat due to these messages. There were clear examples in the interviews where some type of external force influenced user behavior in a positive way including one user who decided to activate a lock screen on his phone due to the interview process. Similarly, Ng and Rahim (2005) suggest we should always remind those around us of the importance of securing our computers. Further results were also found by Agarwal and Anderson (2010) who concluded that people can be influenced by message cues and interestingly positive messages have bigger persuasive influence than negative ones. Overall, subjective norms in the form of peer support and media influence were present in the interviews further validating existing literature.

Home user information security behavior is also influenced by a valuation process where the users value their information that should be protected. Interviewees seem to value their information and depending on the evaluation, security behavior results. Poor information security behavior occurs when users think they have nothing of value to protect. Such practices are worrying since this type of behavior can be risky to other users or service provides. According to the interviews, the earlier mentioned problem of "knowing-doing gap" in organizations then exists in the home context as well further explaining about home user information security behavior.

Finally, skills and awareness on information security matters clearly influence information security behavior. Less skilled users explained in many instances how they simply don't know about certain issues therefore neglecting countering measures that could keep them safer on the internet. Skilled users clearly were able to elaborate in detail about how they practice safe computing in different areas. Yet, sometimes skilled users showed overconfidence and it's not given that skills lead to better information security behavior. In literature the same topic has often been called as self efficacy and similar results have been reached: *high self efficacy contributes to safe computing*. Role of self efficacy have been confirmed in contexts such as protecting home wireless networks (Low et al, 2005), adopting antispyware software (Lee & Kozar, 2008; Liang & Xue, 2010) and in more general settings (Agarwal & Anderson, 2010; Ng & Rahim, 2005).

Overall, new concepts emerged in the study but there was clear relation to past research. For example automation and mandatory safety features is an old subject in the workplace yet it has not being discussed in home context. Interviews also pointed out that while automation can help users they often have to accept and enable it themselves. Responsibility of the user to enable something seemed to lead to neglect in many cases in the interviews. Also, previous research has not discussed how bad experiences could contribute to individual's threat appraisal process and how such experiences could actually be a good thing in the bigger picture of information security. It was also discovered that the "knowing doing gap" of organizations exists in home user context as well since users tend to neglect security when the value of their protected information is perceived to be low. Skills and awareness mostly confirmed past literature and the role of awareness was significant.

7.1 Implications for research

Conducted empirical research was done without any existing theories in mind. Such research has been suggested in literature (Li & Siponen, 2011). Mostly the interviews confirmed a lot of what is already known about the subject. This is in no way a bad thing, on the contrary further evidence in how to influence home user information security behavior gives confirmation to the existing studies. The interviews were able to bring up different concepts in the field of home user information security behavior that can be further researched in relation to existing theories or as independent study subjects.

First, automation and forced measures seem to work well together when it comes to improving information security of individuals. What is unknown is how much users are willing to give up their freedom of choice on the matter and could forced measures be accepted better if awareness of the importance is better explained. Taking out the choice from the user completely is a very drastic option even though the study suggested this is a good way to ensure safe computing. More knowledge is also needed in knowing how much overall se-

curity is due to automation i.e. what would happen if the security was completely in the hands of the users. If there was further support telling forced measures are solely a good thing, it would be easier to justify promotion of forced information security measures as well. In organizational literature Bommer et al. (2010) claims that automation alone has not been sufficient in practice. This sounds very feasible and is probably true in home use context as well. Nevertheless, it's important to know how much automation and forced measures are sufficient and at which point users start to rebel against such drastic and forced measures.

Second, the linkage between bad experiences and threat appraisal in protection motivation theory is an interesting topic. Interviews seemed to confirm there is a linkage but how strong? And does this linkage diminish overtime meaning, does the sense of threat lower when something bad does not happen in a while and does this lead to carelessness. Also, bad experiences lead to higher sense of threat but it is unclear can this knowledge lead to better information security of the wider community. Bad experiences happen and individuals learn from them, but can these events somehow benefit others? Can the often mentioned common sense be distributed to the less skilled users?

Third, some of the less skilled users justified their "poor" behavior due to being unaware of the threats. At the same time users tend to neglect security when information is seen as invaluable and again unawareness of the implications is present. Therefore, it would seem some of the people have not received enough awareness on information security or the importance of the subject has not being made clear enough for the people to listen. Reasons to why such things occur are of great importance. If for example most of the people in Finland use internet frequently it is important to reach the wide audience, not just the computer savvy users. How this can be achieved is a good area of research in the future.

Fourth, it would be interesting to know how someone becomes "savvy" in information security and related behavior. Traditionally one might think that it is the "geeks" who spent hours on their computers that develop better skills but as statistics shows, almost everyone is online these days (SVT, 2014). Yet, this increased use of internet devices does not seem to lead to better information security on every user. Only some develop skills in computer use and information security. Reasons to why this is the case is an interesting topic. This study has contributed on the question already by pointing out the role of bad experiences. Yet more understanding is needed. Could it be possible to learn the process of becoming a safe computer user and repeat it to the wider audience by means of education?

Finally, it seems that friends and other peers can influence user to adopt safety features when done in right fashion. Such behavior should be encouraged but it is unclear how much this type of behavior is happening and how many influence their peers intentionally and often. Most importantly it would be beneficial to know how to encourage safety climate among friends in such matters.

7.2 Implications for practice

Findings from the study have some practical implications to consider. Designing of information systems and devices from security point of view should focus in making the protection mechanisms default and it should be up to the user whether to disable such mechanisms. Not the other way around. The study revealed that such mechanisms are not always automatic and mere suggestions do not lead to better information security. Disabling such mechanisms should not be too easy either to ensure that when it happens, the user probably knows what he or she is doing. This is a job for the security specialists in organizations that design such devices and systems.

Information security related skills and overall low awareness on the topic seems to be a contributing factor in poor behavior. In the study only two interviewees mentioned some type of training that they had received on the matter and neither confirmed it being a big influence in their information security behavior. Such situation is not optimal when the whole cyber-infrastructure should be secured. Warnings on the other hand seemed to reach at least some of the interviewees. Overall, responding to threats is a matter of both skills and awareness. Receiving information about a threat does not work if the user lacks skills to take countermeasures. Based on the study home users should receive training, they should be made aware about the seriousness of the threats and general warnings should always come with instructions in how to counter the threat. Such responsibility is a joint effort of many parties. While younger audience might be easiest to reach in schools, majority of the people can only be informed through public channels such as the internet and public television. Such projects cost money, especially when the information and training should be of high quality to ensure education is more than a passive process of going through a checklist. Safe information security behavior is a continuous proactive effort to constantly keep ones information safe from any kind of threats. As of now, education of the wider public seems to struggle: there seems to be no training to most of the people, people are unaware of the seriousness of the threats or the relating countermeasures, and warnings are not taken seriously enough.

7.3 Limitations

As for limitations, it is unknown whether interviewees reported behavior represents their actual behavior. An interviewee might answer he does not read junk mail or open unknown attachments because he or she is embarrassed to admit occasional lapses in secure behavior. Nevertheless, openness was promoted in the interview situations and it seemed that most of the interviewees were able to report behavior that didn't sound wise even though it might feel embarrassing to them. Another question is whether "more careful and cautious" behavior

means anything at all in practice. It was reported that warnings in the media and bad experiences has influenced users to be more cautious. But what this means in reality is another question.

8 CONCLUSIONS

Information security behavior of individuals seems to puzzle scholars in both workplace and in home context. Employees have trouble complying with set rules and guidelines that enhance the information security of an organization. While employees threaten the valuable information in their organizations, the large population of home users are in position to compromise the whole infrastructure of the internet (Agarwal & Anderson, 2010). Acknowledging the risks that individuals pose in the area of information security this thesis set out to find out more about the phenomenon.

A short overview of the literature in the workplace settings brought up different theories and results that give a better view of what is going on in organizations. While this paper was mainly concerned about home users, the chapter opened up relevant theories and concepts that have been used to advantage in the home research context as well. In short, employees can be influenced by issuing sanctions to policy violations, providing awareness and training to employees, providing facilities so that employees can better comply with given guidelines and convincing employees that the compliance of set policies is not optional but mandatory. Individual employees are affected by factors such as habits, self-efficacy (skills and confidence that provide the ability to comply with policies), moral beliefs and assessment of threat likelihood and severity i.e. threat appraisal.

While literature in workplace settings is thorough and well documented, there is still limited understanding of what motivates home users and how they can be influenced (Agarwal & Anderson, 2010). There are clear differences in the context of home use that need to be acknowledged so that research in this particular context can develop (Li & Siponen, 2011). With the help of literature review of the relevant research as well as interviews conducted with a small group of participants, answers to the research question "what factors influence home user information behavior" were achieved and discussed in detail in the previous chapters of the thesis. In addition some suggestions for further research and practice were introduced.

REFERENCES

Agarwal, R. & Anderson, C. L. (2010). Practising safe computing: a multimethod empirical examination of home computer user security behavioral intentions. MIS *Quarterly,* 34(3). 613-643.

Angermeier, I., Boss, S. R., Boss, R. W., Kirsch, L. J. & Shingler, R. A. (2009). If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems*, (18), 151-164.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, 22(4), 308-313.

Aura, T., Leiwo, J. & Nikander, P. (2000). Towards Network Denial of Service Resistant Protocols. In Eloff, J. H. P. & Qing, S, *Information Security for Global Information Infrastructures*, IFIP TC11 Sixteenth Annual Working Conference on Information Security (p. 301-310). US : Springer-Verlag.

Backhouse, J. & Dhillon, G. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.

Banjara, K., Chen, R., Herath, T., Rao, H. R., Wang, J. & Wilbur, J. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information systems journal*, 24(1), 61-84.

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

Blakely, B., Geer, D. & Mcdermott, E. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms*, NSPW '01 (p. 97-104). New York: ACM.

Bryant, P., Furnell, S. M. & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computer & Security*, 26, 410-417.

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.

D'arcy, J., Hovav, A. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, 49, 99-110.

D'arcy, J., Hovav, A. & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research,* 20(1), 79–98.

Dey, I. (2004). Grounded theory. Teoksessa C. Seale, G. Gobo, J. F. Gubrium & D. Silverman. (toim.), *Qualitative research practice (80-93)*. London: SAGE.

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

Enbody, R., LaRose, R. & Rifon, N. J. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, 51(3), 71-76.

Eloff, J. H. P. & Venter, H. S. (2003). A taxonomy for information security technologies. *Computer & Security*, 22(4), 299-307.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. MIS *Quarterly,* 20(3), 257-278.

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.

Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. In *NSPW '09 Proceedings of the 2009 workshop on New security paradigms workshop* (p. 133-144).

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computer & Security*, 31(1), 83-95.

Gritzalis, D., Kastania, A. & Mylonas, A. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computer & Security*, 34, 47-66.

ISO/IEC 27000:2014. (2014). International standard. Information technology - Security techniques Information security management systems - Overview and vocabulary. Haettu 28.4.2014 osoitteesta http://www.iso27001security.com/html/27000.html

Johnston, A. & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS *Quarterly*, 34(3), 549–566.

Kozar, K. A. & Lee, Y. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*, 45, 109-119.

Larsen, K. R. & Lee, Y. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software. *European Journal of Information Systems*, 18, 177-187.

Lee, S. G., Lee, S. M. & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management* , 41(6), 707–718.

Li, H., Sarathy, R. & Zhang, J. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision support system*, 48, 635-645.

Li, Y. & Siponen, M. (2011). A Call For Research On Home Users' Information Security Behavior. In *PACIS 2011 Proceedings* (p. 1-12).

Liang, H. & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the association for information systems*, 11(7), 394-413.

Low, R., Tan, G. & Woon, I. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In Avison, D., Galletta, D. & DeGross, J. I., *Proceedings of the 26th International Conference on Information Systems* (p. 367-380). Las Vegas.

Mahmood, M. A., Pahnila, S. & Siponen, M. T. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Hawaii International Conference on System Sciences* (p. 156-166). Los Alamitos, CA, IEEE Computer Society Press.

Mahmood, M. A., Pahnila, S. & Siponen, M. T. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, 43(2), 64-71.

Mattord, H. J. & Whitman, M.E. (2012). *Principles of information security*. (4th edition). Course Technology : Cengage Learning.

Nance, W. D. & Straub, D. W. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. MIS Quarterly, 14(1), 45-60.

Ng, B. Y. & Rahim, M. (2005). A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security. In *PACIS 2005 Proceedings* (p. 234-247), 20.

Nist glossary. (2013). *Glossary of Key Information Security Terms*. National Institute of Standards and Technology. Haettu 28.4.2014 osoitteesta http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Pahnila, S., Siponen, M, T. & Vance, A. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*. 49(3–4), 190–198.

Puusniekka, A. & Saaranen-Kauppinen, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu 12.11.2014 osoitteesta http://www.fsd.uta.fi/menetelmaopetus

Rippetoe, S. & Rogers, R. W. (1987). Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat. *Journal of Personality and Social Psychology*, 52(3), 596-604.

Siponen, M. T. & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS *Quarterly*, 34(3), 487–502.

Siponen, M. T. & Vance, A. (2013). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *Information Systems Research,* 1-17.

Straub, D. W. (1990). Effective IS security: an empirical study. *Information Systems Research*, 1(3), 255–276.

Suomen virallinen tilasto (SVT). (2014). Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. Helsinki: Tilastokeskus. Haettu 11.11.2014 osoitteesta http://www.tilastokeskus.fi/til/sutivi/2014/sutivi_2014_2014-11-06_tie_001_fi.html

Warkentin, M. & Willison, R. (2013). Beyond deterrence: an expanded view of employee computer abuse. MIS *Quarterly*, 37(1), 1-20.

Bommer, W., Straub, D. & Workman, M. (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.