Sanna Kinnunen

EXPLORING DETERMINANTS OF DIFFERENT INFORMATION SECURITY BEHAVIORS

UNIVERSITY OF JYVÄSKYLÄ
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS
2016

ABSTRACT

Kinnunen, Sanna
Exploring determinants of different information security behaviors.
Jyväskylä: University of Jyväskylä, 2016, 60 p.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

Aim: The aim was to introduce new explanatory construct, namely illegitimate tasks from Stress-as-Offense-to-Self Theory (SOS), to better understand information security behavior (ISB). In addition, more commonly used constructs from Deterrence theory (DT) and Protection Motivation Theory (PMT) were used to explain ISB. This study also investigated several behaviors separately to evaluate the generalizability of the behavioral determinants. **Methods:** Four ISBs, namely general ISP compliance (ISP), not copying sensitive information to the unsecured USB drive (USB), locking or logging out from the computer (LOG), and not writing down passwords (PSW). Formal and informal sanctions from DT, threat and coping appraisal, as well as fear, from PMT, and illegitimate tasks from SOS were included as determinants of ISB. The survey method was used to data collection, and each participant answered to one behavior-specific questionnaire. There were 119 respondents to the ISP, 111 to the USB, 118 to the LOG, and 112 to the PSW questionnaires. 55,5% of the 460 participants were male, and 62,2% belonged to the age group of 20-30 years. Most of the participants (56,3%) had 1-7 years of work experience and they were technologically savvy. Confirmatory factor analysis and hierarchical linear regression analysis were used in the analyses, and analysis strategy was applied separately for each of the four ISBs. **Results:** DT, PMT, and SOS, as well as control variables, explained more than half of the variance (51,1-57,9%) in all of the behaviors, namely ISP, USB, LOG, and PSW. Illegitimate tasks had a relatively strong negative association with two of the ISBs indicating that they function as a determinant of ISB and should be considered in the future research of ISB. Illegitimate tasks also added explanatory power to the models containing sanctions from DT and appraisals from PMT. Illegitimate tasks were the strongest determinant of ISP and LOG. Although illegitimate tasks had a significant association with two of the ISBs, PMT contributed the most strongly to explaining different ISBs. Rewards and costs were the most prominent determinants of behavior and they also correlated highly with illegitimate tasks. This association can be theoretically explained and understood by SOS which addresses the effects of task evaluation on one's self-image and relationship with the organization one works at. Of the other constructs of PMT, fear and threat appraisal were significant predictors of LOG and USB, respectively, while response efficacy and self-efficacy predicted ISP. According to the findings of this study, sanctions from DT were not significant predictors of any of the ISBs. **Conclusions:** ISB has complex and multiple determinants that differ depending on the behavior in question. Findings related to a certain form of behavior are not necessarily generalizable to explaining other behaviors. This should be taken into account when planning research designs and practical procedures for information security management.

Keywords: Information security behavior, Deterrence Theory, Protection Motivation Theory, Stress-as-Offense-to-Self Theory

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

The use of information systems (IS) has brought many advantages to organizations but there are also risks when knowledge is handled with IS. Prominent threats are not only cyber criminals that infiltrate organization's systems but also the personnel of the organization that does not follow company information security policy (ISP). It is estimated that over half of information security breaches are due to employees' inadequate ISP compliance (e.g., Dhillon & Moores, 2001). It is important to understand the motives behind information security behavior (ISB) to be able to influence it in a way that supports ISP compliance.

ISB has been explained by different theoretical models of which two frequently used are Deterrence Theory (DT) (Gibbs, 1975) and Protection Motivation Theory (PMT) (Rogers, 1975; Maddux & Rogers, 1983). DT focuses on the role of formal and informal sanctions, and PMT introduces threat and coping appraisals as mechanisms determining behavior. However, even by combining both of these theories only about half of the variance of ISB can be explained (see e.g., D'Arcy, Herath, & Shoss, 2014; Herath & Rao, 2009b) which indicates that additional explanatory constructs are needed. Recently in the field of psychology, Stress-as-Offence-to-Self theory (SOS) (Semmer, Jacobshagen, Meier, & Elfering, 2007) has explained how tasks that are perceived to be either unreasonable or unnecessary (i.e. illegitimate) can lead to counterproductive work behavior (Semmer, Tschan, Meier, Facchin, & Jacobshagen, 2010). ISP violations are examples of counterproductive behavior and it is possible that illegitimacy of the tasks explains why people do not act securely at work. The present study investigates if illegitimate tasks are able to explain the additional variance of ISB when it is used together with constructs of DT and PMT.

In addition to not being able to account for the majority of the variance in ISB, empirical studies of the role of DT (e.g., Cheng, Li, Li, Holm, & Chai, 2013; Herath & Rao, 2009a; Li, Zhang, & Sarathy, 2010) or PMT constructs (e.g., Kim, Yang, and Park, 2014; Vance, Siponen, and Pahnila, 2012; Workman, 2009) in explaining ISB have yielded mixed results. In some studies, certain associations are found and in others, these associations can be insignificant or contradictory to theoretical expectations. In these studies, a general measure of ISB have been used (e.g., general ISP compliance), and it is possible that by combining all the ISBs to the same measure essential information is lost. Contradictory findings of the previous studies could be due to variation between different ISBs rather than reflections of problematic research designs or sample-specific discrepancies. For example, locking computer while leaving the workstation or not writing down passwords can have different determinants and

when studies ask about general behavior, the respondents combine their views. This way the results may vary because the respondents have focused on different behaviors while answering. The need for context-specific research have been outlined in recommendations for future information security research (e.g., Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville, 2013). The present study takes into account the context by investigating behavior-specific determinants.

The contribution of this study is to present new theoretical construct, namely illegitimate tasks, to understand ISB. In addition, this study will use different behaviors to better illuminate the generalizability of behavioral determinants. This can possibly help to understand contradictory findings of previous studies using DT and PMT to explain ISB. In practice, this kind of information can be used to enhance information security management by addressing people's underlying motives for not acting securely in different situations. This thesis will first define ISB and how it is related to the larger context of information security management. Next, it will present each of the used explanatory theories and previous research of these in relation to ISB. Hypotheses for the present study are based on the three theories and are presented in the literature review and in methods. Measures, participants and procedure, as well as analysis strategy are reported in the methods section, and measurement validity and reliability assessment are also assessed in the methods. The results of the study follow methods, and they are evaluated and reviewed in relation to previous research in the discussion. The discussion also provides limitations and implications for future research and practice.

1.1 Information Security Management and Behavior

1.1.1 Information Security Management

The importance of information security has increased since information security violations are becoming more and more common (Stanton, Stam, Mastrangelo, & Jolton, 2005). Information security management can be defined as the protection of information confidentiality, integrity, and availability through policies, user training, and technology (Whitman & Mattord, 2013). Information security management should be a part of the daily operations of the organization. Information security management includes the following areas: management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies, and compliance enforcement mechanisms; all of which are used to guarantee information security of the company (von Solms, 2005).

von Solms (2005) also divides information security management to operational management and compliance management. Operational management consists of technical solutions for security management and the creation of ISP and awareness programs for educating employees about security issues. Compliance management deals with issues like the level of information security knowledge of employees, the availability, completeness and compliance of ISP, and the risks related to noncompliance of ISP. Both of these aspects need to be considered when conducting good information security management (von Solms, 2005). However, in many companies, information security management does not fulfill these requirements, because it is not realized that security management is a complicated matter that includes

many business and people related issues in addition to technical solutions (von Solms & von Solms, 2004).

An integral part of good information security management is information security policy (ISP) that is defined as a collection of rules and regulations that give guidance in how information security is managed in the organization (Baskerville & Siponen, 2002; Thomson & von Solms, 2005). ISP can have a collection of law-based and industry-specific requirements and specify both technical and non-technical aspects of information security management. Siponen and Willison (2009) suggest that information security guidelines should be evaluated based on their scope of the application and the type of evidence for their use. It is important to base the practices on empirical research of their effectiveness and to understand which guidelines are universal and which are specific for certain environments or situations. With good ISP and management of its use, many security threats and challenges can be dealt proactively and effectively.

1.1.2 Information Security Behavior (ISB)

Crossler et al. (2013) identified five integral themes for future information security research: (1) understanding insider deviant behavior and differentiating it from misbehavior and oversight, (2) defining different types of hackers and determining their motives, (3) improving information security compliance by determining what kinds of incentives and threats are useful motivators in different situations, (4) cross-cultural research, and (5) dealing with data collection and measurement issues. In the contemporary work context, the end user security management is one of the most essential points since employees' behavior have been identified as the biggest threat to organization's information security (Puhakainen, 2006). Over half of information security breaches in the organizations are estimated to be due to employees' inability to follow ISP (Dhillon & Moores, 2001; Stanton et al., 2005).

Because of the significance of employees' ISP violations, a vast amount of research has been conducted to understand motives and reasons behind this phenomenon. ISP compliance is a part of information security behavior (ISB) that refers to how people act when faced with information security issues. Stanton et al. (2005) have classified different forms of end user behaviors based on the expertise required by the action and intentions behind the action. Malicious intentions combined with high expertise is intentional destruction (e.g. stealing company's secrets) and can be costly for the company whereas malicious intentions with low expertise is detrimental misuse (e.g. spamming email) which can cause inconveniences but has a low impact on the company. Neutral intentions with either high or low expertise are defined as dangerous tinkering (e.g. sharing network connection outside the firm) and naive mistakes (e.g. using bad passwords), both of which can be harmful to the organization. Last two classes are driven by beneficial intentions, which combined with high expertise results in aware assurance (e.g. detecting security threats), while beneficial intentions with low expertise results in basic hygiene (e.g. complying with ISP).

As can be seen from the categories of Stanton et al. (2005), ISB can take different forms and be driven by different intentions. Siponen and Vance (2010) report most cited ISP violations to be failing to lock or log out from workstations, storing written-down personal passwords in visible places, sharing passwords with colleagues and friends, transferring sensitive data to the unsecured USB drive, revealing confidential information to outsiders, disabling

security configurations, using laptops carelessly outside the company premises, sending confidential information unsecured, and creating easy-to-guess passwords. These do not necessarily reflect malicious intentions, and because of this, other explanations for behavior must be sought to understand ISB. ISB is considered to be affected by various social, person-, and company-related factors that can be divided between the user's understanding of what is expected from them in relation to information security, and their willingness to act according to these expectations (Abraham, 2011; Leach, 2003). In the organization, the understanding of expectations is affected by values, policies, and procedures of the organization; the behaviors of management and colleagues; and user's basic knowledge of information security issues and their decision-making skills. On the other hand, the willingness to comply is affected by employees' own values and standards, their psychological contract with employers, and the effort required by compliance (Abraham, 2011; Leach, 2003). These and a multitude of other factors have been defined in different models of ISB and two of the most used models are presented below.

In modeling research, ISB has been usually studied using different behavioral scenarios and then combining scenario-specific information to form general models of ISB (see e.g., D'Arcy et al., 2014; Siponen & Vance, 2010). However, it is possible that determinants of behavior vary with different behaviors. Of the categories reported in Siponen and Vance (2010) writing passwords down and transferring sensitive information to unsecured USB drives, for example, are different types of behaviors and are possibly driven by different intentions and motivations. By combining the information from numerous ISBs to the same model, it is possible that information of the behaviors is lost in the process. For example, if a certain motivator is significant for writing down passwords but not at all for the unsecured use of USB drives, it could not appear to be significant in the general model. To better answer the challenges that Crossler et al. (2013) stated for information security research, it is important to investigate different types of behavior to ascertain if the determinants of ISB are general or more context-specific. Context-specific research could also help to understand contradictory research findings related to certain determinants.

1.2 Deterrence Theory (DT) and ISB

1.2.1 DT in the Information Security Field

Deterrence theory (DT) is one of the most popular theories to explain the behavior of individuals in the information security field, and it has even been the most cited theory in this field (Siponen, Willison, & Baskerville, 2008). DT is adopted from criminology and originally it has focused on formal sanctions, such as imprisonment and fines, as motivators for deterring from illicit acts (Gibbs, 1975). According to Gibbs (1975) the perceived severity, certainty, and celerity of sanctions have an effect on what degree a person deters from an illicit action. The severity of sanctions refers to the degree of punishment if caught in illicit acts. For example, in the information security context, being scolded due to a violation is less severe than being fired because of it. The certainty of sanctions depicts the probability of being punished; for example, the certainty of sanctions can be either high or low depending on the surveillance of employees in a certain company. The celerity of sanctions refers to the swiftness of

being punished, i.e. does the sanction follow the action immediately, or with delay. All of these factors can be considered when determining how sanctions affect ISB. For example, if both the certainty and the severity of sanctions are considered to be high, a person could be more likely to handle information securely.

Traditional DT has been extended to include informal sanctions, for example in the form of social or self-approval, as potential determinants of action (Piquero & Tibbetts, 1996). Self-approval refers to a person's view of oneself and one's actions and is accompanied by one's values and moral standards. Social approval, on the other hand, depicts how others view the person and evaluate their actions. The disapproval of friends and colleagues, as well as feeling shame and disappointment duet to one's actions, can have an impact on the choice to deter from illicit acts (Paternoster & Simpson, 1996). In the information security field, informal sanctions can include losing the respect of one's colleagues and supervisor, or even jeopardizing one's promotion prospects (Siponen & Vance, 2010). Contemporary DT considers that both formal and informal sanctions are important when the person decides how to act in a certain situation (Pratt, Cullen, Blevins, Daigle, & Madensen, 2006). The person considers costs and benefits of actions and the probability of either of them realizing before choosing the way to act. In general, this theory is applied to information security context by assuming that formal and informal sanctions in the organization deter employees from violating information security guidelines of the organization. It is assumed that more severe and certain sanctions are connected to more secure ISB.

1.2.2 Empirical research on DT and ISB

Although DT has been widely applied in the information security field, empirical tests of its assumptions have yielded an incomprehensive picture of the effect of sanctions on information security behavior of the users (see e.g., D'Arcy & Herath, 2011). One of the first scholars using DT in information security field, Straub (1990) noticed that countermeasures against information security violations decreased the amount of computer abuse in the workplace. After this, studies have found a different degree of support for the importance of both formal and informal controls in determining ISB. D'Arcy and Devaraj (2012) observed that certainty and severity of punishments were negatively associated with technology misuse intentions. Guo and Yuan (2011) observed that personal self-sanctions and workgroup sanctions predicted intentions to comply with ISP, but organizational sanctions were not significant predictors after the other two were added.

Many studies have found support for the significance of only perceived severity or perceived certainty of sanctions. Cheng et al. (2013) noticed that perceived severity of sanctions influenced significantly ISP violation intentions, and of the sanctions especially social pressures exerted by co-worker behaviors and subjective norms were significant predictors of behavior. D'Arcy, Hovav, and Galletta (2009) found that awareness of information security related issues increased the perceived amount of severity and certainty of sanctions, but only the severity of sanctions was associated to intentions to deter from IS misuse intentions. Contrary to these findings, Li et al. (2010) observed that perceived certainty of getting caught was positively associated with ISP compliance intentions, but perceived severity of sanctions was not. Kankanhalli, Teo, Tan, and Wei (2013) did also not find the association between punishment severity and perceived IS security effectiveness. However, the magnitude of deterrence efforts was positively associated with security effectiveness. Herath & Rao (2009a) found

support for the importance of perceived certainty of sanctions in predicting ISP compliance intentions. Contrary to expectations, in their study ISP compliance was less likely when the perceived severity of sanctions was high. There are not that many studies of the importance of celerity of sanctions in the field of information security, but it has been included in the general factor of deterrence-related items (e.g., Siponen, Pahnila, & Mahmood, 2010). In the study by Siponen et al. (2010) deterrence as a whole was positively associated with actual compliance with ISP.

Still other studies have not found an association between any form of sanctions and employee behavior, especially if more explanatory factors are added to the models (Lee, Lee, & Yoo, 2004; Siponen & Vance, 2010). Lee et al. (2004) noticed that strong deterrence factors in the organization did not explain intention to use protective measures against information security breaches while the investment in and effectiveness of physical security system were predictors of secure use intentions. Furthermore, the role of formal and informal sanctions in explaining ISB became insignificant when neutralization techniques (i.e. techniques used to disvalue the importance and necessity of complying with ISP) were added to the model (Siponen & Vance, 2010). These findings show that the role of sanctions is not consistent across the studies and that based on these results it is difficult to make clear conclusions about the importance of sanctions in explaining ISB. It is possible that these discrepancies are due to differences between behaviors in a way that sanctions deter people from certain actions but not from others.

Recent studies have indeed shown that the significance of sanctions in determining employee behavior depends on contextual factors (D'Arcy and Hovav, 2009; Hovav and D'Arcy, 2012). D'Arcy and Hovav (2009) noticed that computer savvy employees, as well as employees doing more remote work, are less deterred from unsecured behaviors because of SETA programs. They also noticed that different countermeasures, namely awareness programs (SETA), security policies, and computer monitoring, were differently associated with behavioral intentions. The SETA program was associated with lower unauthorized access intention, while security policies and computer monitoring were associated with lower unauthorized modification intention. In addition, Hovav and D'Arcy (2012) observed that the effectiveness of certain countermeasures, namely security policy statements, security education, training, SETA programs, and computer monitoring were different in U.S. and Korean samples, indicating cultural effects. Based on the importance of context, it is possible that sanctions are more prominent determinants in certain situations than in others. However, these studies have not investigated different behaviors as possible reasons for differing findings.

D'Arcy and Herath (2011) recognize the importance of context when suggesting future directions for the research of DT. They propose that the effect of formal and informal sanctions should be studied in relation to different types of ISB to better understand the generalizability of the theory. It is possible that for example formal sanctions have a different role in explaining someone writing down hard-to-remember passwords, and in not logging out from their computer while leaving the workstation for a brief period. These possible differences between behaviors are the focus of the present study. If the role of the formal and informal sanctions varies between behaviors this can help to understand the contradictory findings of previous studies. Although the present study focuses on investigating differences in determinants of various ISBs, basic hypotheses of the connections between sanctions and behavior are drawn from the theoretical expectations. It is assumed that both higher formal and informal sanctions deter people from illicit actions (e.g., D'Arcy & Herath, 2011; Pratt et

al., 2006). In the present study, these assumptions are tested separately for different behaviors. By testing general hypotheses in different contexts, it is possible to determine how generalizable the theoretical expectations are and if it is reasonable to apply the theory to any situation. The following general hypotheses can be formulated based on DT:

H1: Higher severity of formal sanctions is positively associated to secure ISB.
H2: Higher certainty of formal sanctions is positively associated to secure ISB.
H3: Higher severity of informal sanctions is positively associated to secure ISB.
H4: Higher certainty of informal sanctions is positively associated to secure ISB.

1.3 Protection Motivation Theory (PMT) and ISB

1.3.1 PMT in the Information Security Field

Another theory that is often used in the information security field is Protection Motivation Theory (PMT), which explains how people respond to threats (Rogers, 1975). It was originally developed to explain the effects of fear appeals on behavior. Fear appeals refer to persuasive messages that arouse fear (Witte & Allen, 2000). Since the first conceptualization of PMT, it has been revised and new explanatory components have been added (Floyd, Prentice-Dunn, & Rogers, 2000; Maddux & Rogers, 1983). According to PMT, coping with threat situations and fear appeals is determined by two processes, threat appraisal and coping appraisal (Floyd et al., 2000; Rogers, 1975). Threat and coping appraisal are described as cognitive mediating processes that together lead to protection motivation which in turn acts as a motive for a chosen coping mode. Threat appraisal assesses the determinants of maladaptive behavior while coping appraisal focuses on the possibilities to avert the threat or to cope with it (Floyd et al., 2000). As indicated earlier the outcome of these appraisal processes is the formation of the decision to initiate, inhibit, or continue a certain behavior. In the information security context, the result of these processes could be to either follow the ISP of the company or to refrain from it.

Threat appraisal refers to the evaluation of how threatened one is in a certain situation. Fear appeals, which are the starting point for the threat appraisal, can be aroused by information acquired via environmental cues and from previous experiences (Floyd et al., 2000). In the information security field, employees acquire information about security-related issues from various sources: for example, ISPs, memos, supervisors, and colleagues. They may also have certain assumptions of information security based on their level of expertise with it or their previous experiences of security threats. This information helps when evaluating the threat by the probability that it actualizes (vulnerability) and by the severity of the consequences if it occurs (severity) (Floyd et al., 2000; Rogers, 1975). Evaluations of vulnerability and severity lead to different levels of fear which motivate the selection of an adaptive response. Threat appraisal is also affected by the rewards associated with the certain type of behavior, and adaptive or maladaptive rewards cause respective behavior. In the information security context, vulnerability to the security threat and its severity can be evaluated from the perspectives of both individual and organization (Herath & Rao, 2009b). For example, an individual can perceive a certain security threat to be significant for the organization but not

fear-evoking for oneself. If this kind of evaluation is accompanied by the maladaptive reward of saving one's own time and effort by not engaging in secure behaviors, the unsecured behavior is more likely.

Coping appraisal includes the assessment of the efficacy of possible coping methods in dealing with the threat (response efficacy), and the evaluation of one's own capabilities to respond to threats and complete coping actions (self-efficacy) (Floyd et al., 2000; Maddux & Rogers, 1983). Positive evaluations of response efficacy and self-efficacy are likely to increase the probability of an adaptive response to the threat. In addition to efficacy evaluations, response costs are assessed during the coping appraisal. These costs can be in any form: for example, monetary, time, effort, or personal costs (Floyd et al., 2000). If the costs of responding adaptively to the situation are high, they decrease the probability of adaptive behavior. In the information security context, a person can evaluate the efficacy of the organization's systems and policies in handling security threats and one's own ability to use information systems securely. They can also connect different kinds of costs to complying with ISP, for example, an excessive need for time and effort to understand the rules and comply with them. These evaluations can then either compensate the effects of threat appraisal process, lead to an adaptive response, or weaken the perceived ability to react adaptively to the threat. In general, threat and coping appraisal processes lead jointly to protection motivation and affect the selection of behaviors in a certain situation, for example, the choice to follow ISP or use information systems securely.

1.3.2 Empirical research on PMT and ISB

Several studies have found support for the assumptions of PMT in the field of information security. However, there are also studies where some of the expectations are not supported or where the results oppose theoretical hypotheses. Workman, Bommer, and Straub (2008) noticed that perceived vulnerability and severity, as well as response efficacy and self-efficacy, explained both the subjective and objective omissive behaviors of employees as the theory assumes. Furthermore, Ifinedo (2011) found support for the importance of most the constructs of PMT, except for response cost, in explaining ISP compliance intention. However, contrary to expectations the perceived severity of threat decreased the compliance intentions instead of increasing them. The perceived vulnerability has also had an unexpected negative impact on a variety of security practices while greater perceived severity predicted practices as expected in the theory (Crossler & Bélanger, 2014). They also noticed that greater response efficacy and self-efficacy predicted better security practices, but response cost was not a significant predictor. There have been studies where response efficacy has not been a significant predictor of ISP compliance intention, while severity, vulnerability, and self-efficacy have (Siponen, Mahmood, and Pahnila, 2014).

Furthermore, Workman (2009) noticed that greater personal vulnerability to security threats and greater self-efficacy resulted in more positive attitudes towards security surveillance, as well as did greater perceptions of company security efficacy. In this study, perceived severity became significant only in the situation where perceptions of organizational procedural justice were high. In comparison, perceived severity but not perceived vulnerability was a significant predictor of ISP compliance intention in the study by Vance et al. (2012). Their study also supported the significance of rewards and response costs (negative association) and response efficacy and self-efficacy (positive association) in explaining compliance

intentions. Self-efficacy has explained significantly secure behavioral intentions almost in every study, but interestingly in the study by Kim et al. (2014), this relationship was not detected. High self-efficacy regarding one's own capability to take care of security-related issues can also have a negative effect on adoption intention: for example, email screening self-efficacy (internal coping appraisal) was negatively associated with the intention to adopt email authentication services (Herath, Chen, Wang, Banjara, Wilbur, & Rao, 2014). In their study, threat appraisal and external coping appraisal were positively associated with the intention to adopt authentication services.

It has also been noticed that threat and coping appraisal processes have an influence on each other. High perceived threat severity predicted lower self-efficacy and lower evaluation of response efficacy, which in turn increased behavioral intentions to act securely (Johnston & Warkentin, 2010). However, perceived vulnerability to the threat was not associated with self-efficacy or response efficacy. Although most of the studies have focused on the relationship between appraisal processes and chosen behavior, there are a few studies that have added preceding factors from the PMT to their research models. Siponen, Pahnila, and Mahmood (2006) found that normative expectations of colleagues and the visibility of system use in the company affect threat and coping appraisals which in turn predict compliance intentions. Furthermore, routinized forms of past behavior (i.e. habits) were found to be important information sources affecting threat and coping appraisals (Vance et al., 2012).

In summary of the research on PMT in the information security field, all of the constructs in PMT have been noticed to be significant predictors of security intentions and behaviors in some studies, but not in others. It is possible that the discrepancy between findings is due to the differences in their contexts: certain constructs could be important with regards to certain behaviors while other factors are needed with different behaviors. By combining the variety of ISBs into the same explanatory model, the results can differ based on behaviors used in each study. It is possible that the results would be clear and concise if context-specific factors would be taken into account in interpreting results. A few studies have indeed found differences in the importance of threat and coping appraisals in different contexts. Lee and Larsen (2009) investigated the effects of threat and coping appraisals on executive's decisions to adopt anti-malware software for their organization, and found that threat appraisal was more central for the adoption intention of IS experts and IT-intensive industries while coping appraisal was more important for non-IS experts and non-IT intensive industries. Threat appraisal has also been the stronger motivator for adopting anti-plagiarism software in universities than coping appraisal (Lee, 2011).

However, as with DT, the different behaviors have not been studied as contextual factors until recently. Boss, Galletta, Lowry, Moody, & Polak (2015) used all of the constructs of PMT in explaining two kinds of security behaviors, namely back-up intentions and anti-malware software use intentions. Their results of the significance of explanatory factors differed in a few respects according to security behavior in question and also in relation to the level of fear appeal manipulation. When all the fear appeal manipulations were combined, only the perceived severity of threat (which increased the probability) and response costs (which decreased the probability) explained back-up intentions while anti-malware software use intentions were predicted by response efficacy (increased the probability) and response costs (decreased the probability). In both models, intentions predicted actual behaviors. However, in the high fear appeal manipulation, all of the constructs in PMT were significant explanatory factors for both back-up intentions and anti-malware software use intentions (Boss et al.,

2015). In the low fear appeal manipulations, only response costs and threat vulnerability were significant predictors of back-up intentions; while for software use intentions all the constructs were significant, except threat severity and threat vulnerability as direct predictors of intentions. The study by Boss et al. (2015) shows that explanatory factors could differ for different types of security behaviors and this venue warrants further investigation.

The present study uses several ISBs to investigate the differences in determinants but for the basis of the analyses a few general hypotheses are formulated. These hypotheses are based on assumptions of PMT that expect that threat and coping appraisal, as well as fear, determine together the protection motivation which leads to behavior (Floyd et al., 2000; Rogers, 1975). Generally, higher appraisals and higher fear are expected to lead to greater protection motivation and this way to the higher amount of protective behavior. In the field of information security, a higher amount of protective behavior is depicted in secure ISB. In the present study, the theoretical expectations are tested for different behaviors. By testing general hypotheses in various contexts, it is possible to determine how generalizable the theoretical expectations are and if it is reasonable to apply the theory in all situations. The following general hypotheses can be formulated based on PMT:

H5: Higher threat severity is positively associated to secure ISB.
H6: Higher threat vulnerability is positively associated to secure ISB.
H7: Higher maladaptive rewards are negatively associated to secure ISB.
H8: Higher fear is positively associated to secure ISB.
H9: Higher response efficacy is positively associated to secure ISB.
H10: Higher self-efficacy is positively associated to secure ISB.
H11: Higher response costs are negatively associated to secure ISB.

1.4 Combining DT and PMT in Explaining ISB

PMT has also been applied in combination with DT to explain ISB. Pahnila, Siponen, and Mahmood (2007a) observed with data from 245 Finnish employees that threat appraisal explained attitudes towards complying with ISP while coping appraisal did not. In addition to threat appraisal, facilitating conditions explained attitudes. Attitudes towards complying explained intention to comply, as did normative beliefs and habits. However, sanctions did not have additional explanatory power for intentions. Finally, intention to comply and information quality explained actual compliance, but rewards for complying did not. In this study, the variance explained by the model was relatively low for attitude towards complying (8,0%) but notably high for the intention to comply (64,9%) and for actual compliance (79,3%). The high explanatory power of intention and actual compliance was mostly due to attitudes towards complying and compliance intention being part of the models.

Pahnila, Siponen, and Mahmood (2007b) and Siponen, Pahnila, & Mahmood (2007) (see also Siponen, Pahnila, & Mahmood, 2010) utilized the same data set of 917 employees from four different companies. Siponen et al. (2007) noticed that both threat and coping appraisal explained intention to comply with ISP and that sanctions explain actual compliance with ISP. In addition, intention to comply explained actual compliance. Their research model explained 71 % of actual compliance, the largest share of which was due to the intention to

comply. Pahnila et al. (2007b) added components from other theories besides DT and PMT: response efficacy was not a significant explanatory factor for intention to comply in their model, while self-efficacy and threat appraisal were, just as in the study by Siponen et al. (2007). Of the added explanatory components, normative beliefs of colleagues and visibility of other's system use were significant for intention to comply (Pahnila et al., 2007b). Their model explained 72 % of intention to comply. Intention to comply and sanctions explained actual compliance, as in Siponen et al. (2007). Added rewards did not yield significance. Based on these studies, the importance of components of DT and PMT can change when new constructs are added to the model.

Herath and Rao (2009b) have also combined DT and PMT in their study of 312 employees from 78 different organizations. They noticed that perceived severity of the threat, but not perceived certainty of it, explained security breach concern level which in turn explained attitudes towards security policy. Furthermore, response efficacy, self-efficacy, and response costs explained ISP attitude. However, security policy attitude did not predict ISP compliance intention, while self-efficacy on its own did. In addition, detection certainty was positively associated with ISP compliance intention, and contrary to the expectations of DT, punishment severity was negatively associated with it (Herath & Rao, 2009a). The research model also contained organizational commitment which was positively associated with both response efficacy and compliance intention as well as resource availability which was positively associated to self-efficacy. Subjective and descriptive norms also explained compliance intentions, as did gender of the demographic variables. The whole model explained 47 % of ISP compliance intention and 48 % of ISP attitude.

Although the explanatory levels in the cited papers are relatively high, this is mostly due to the adding up attitudes towards complying or intention to comply as explanatory factors for actual compliance. New constructs in addition to those from DT and PMT are needed to understand what explains ISB. In the field of work and organizational psychology, a new theory has been applied to explain counterproductive work behavior (Semmer et al., 2010), of which unsecured ISB could be an example. This theory is presented next and used in the present research to contribute to the knowledge of behavioral determinants essential in the information security field.

1.5 Stress-as-Offense-to-Self Theory (SOS) and ISB

1.5.1 Presenting SOS

The present study intends to offer a new perspective to ISB by including Stress-as-Offense-to-Self theory (SOS) (Semmer et al., 2007; Semmer et al., 2015) from the field of work and organizational psychology. The roots of SOS are in role theory and justice theory, and it addresses the importance of self-esteem, reciprocity, and fairness in the creation of stress experiences. According to SOS, people strive to preserve their self-worth and to maintain a positive self-image. Threats to the self-image are seen as core activators of stress reactions in different situations and motivators for counterproductive behavior. Threats to self include threats to personal self-evaluation of oneself as a human being, and threats to social esteem, which refers to how other people evaluate oneself (Semmer et al., 2007). These evaluations

have been shown to be interrelated (e.g., De Cremer & Tyler, 2005), although it is possible that only one or the other is affected in certain situations. SOS also recognizes the boosters of personal and social esteem, like pride and appreciation, and expects these to diminish stress experiences (Semmer et al., 2007).

The threat to personal self-esteem rises in the situations where a person experiences that one cannot live up to the expectations posited to oneself (Tracy & Robins, 2004). For example, in the work context employees may experience that they are unable to perform work on the level that they expect of themselves because of busy schedules or organizational demands. Threats to social esteem are caused by disrespect experienced from other people (Semmer et al., 2007), for example in the form of direct attacks towards one's performance and the person, or indirectly by not informing the person in time for them to be prepared for difficult situations. The present study focuses on a third way of undermining social esteem since this is probably the most salient in understanding ISB, namely illegitimate tasks.

Illegitimate tasks refer to assignments that are perceived to be unreasonable or unnecessary (Semmer et al., 2007; Semmer et al., 2015). Illegitimate tasks should be distinguished from the uncomfortable tasks that are perceived to be part of one's job description, like telling bad news to patients in the medical care. These are not experienced to be significant stressors (Peeters, Buunk, & Schaufeli, 1995). Illegitimate tasks are experienced to be additional burdens that can cause significant amounts of stress. Unreasonable tasks are tasks that are not appropriate for one's job description or professional role and should be done by someone else (Semmer et al., 2007; Semmer et al., 2015). For example, when a teacher uses a considerable share of their day by filling out various administrative forms, one can experience that participation in such activities was not the objective of one's extended education and that one's competence would be better utilized in teaching students. On the other hand, unnecessary tasks are tasks that employees perceive to be redundant and that should possibly not be done at all. For example, when a researcher has to manually copy files from one system to the other because they are needed in both systems but the systems are unable to complete the transfer automatically. Having illegitimate tasks can be experienced as an indirect sign of disrespect from the organization towards the employee (Semmer et al., 2015). They convey a social message of the organization not caring for the employees, and in this way diminish the employees' motivation to strive for the goals of the job and to be a good organizational citizen. This kind of message could be an important factor in explaining why employees are reluctant to follow ISP or improve information security by their actions.

1.5.2 Applying SOS to Explain ISB

Approximately a third of all tasks were perceived to be illegitimate in a survey by Semmer's research group (see Semmer et al., 2007) which indicates that a considerable amount of work time is spent doing tasks that are not meaningful to the employees. Björk, Bejerot, Jacobshagen, and Härenstam (2013) noticed in their study of 28 different organizations that 10% of the variance in illegitimate tasks could be explained by organizational factors. More illegitimate tasks were reported in organizations that had competition for resources, unfair resource allocation, and an obscure decision-making structure. These kinds of conditions could also be important when understanding why employees do not act securely even though there would be sanctions for not following ISP or they would feel themselves be competent to act securely on their own. For example, in a situation where one's department is competing for

resources with other units and where more productive units are allocated more resources, demand to comply with ISP could be experienced as unreasonable on the top of the other tasks, as familiarizing with ISP takes time and effort. A recent survey answered by 2800 employees indicated that key reasons for not acting securely at the workplace and not following ISP were the inconvenience of following the policies and being too busy to concentrate on them (Cisco Systems, 2011), which supports the possibility of SOS to add explanatory power to the previous models of ISB.

In other fields, illegitimate tasks have been linked to counterproductive work behavior and to other detrimental costs for the organization. Counterproductive work behavior refers to the behavior which is intended to be hurtful either to the organization or certain members of it (Spector & Fox, 2002). It can manifest itself as revenge, delinquency, or antisocial behavior, but most noticeably by deviance. Examples of deviance include returning assignments late, not putting effort into the tasks, or ignoring some tasks (e.g., ISP compliance) altogether. Illegitimate tasks have been related to these kinds of counterproductive work behaviors, even when other factors commonly related to counterproductive behavior, like effort-reward imbalance or organizational justice, have been controlled for (Semmer et al., 2010). Illegitimate tasks have also been related to resentment towards one's organization and dissatisfaction at work (Björk et al., 2010; Stocker, Jacobshagen, Semmer, & Annen, 2010). Semmer et al. (2015) have even shown that resentment and irritability are predicted by illegitimate tasks, rather than the other way around. It has also been noticed that unreasonable tasks directly decreased volunteers' intention to remain at the job and that unnecessary tasks reduced the volunteers' personal motivation towards the job (van Schie, Güntert, & Wehner, 2014). The effects of unnecessary tasks were more detrimental to those volunteers who were committed to the organization. All these studies indicate that illegitimate tasks have a considerable impact on how employees act at work, especially in cases of deviant or counterproductive behavior, of which unsecured ISB is an example.

In addition to the associations between illegitimate tasks and work-related behavior, illegitimate tasks are related to stress experiences and lower self-esteem, as expected by the theory (see e.g., Björk et al., 2013; Semmer et al., 2015). Illegitimate tasks have been linked to increased cortisol (stress hormone) levels when personal health resources are slow (Kottwitz, Meier, Jacobshagen, Kälin, & Elfering, 2013) and to fragmented sleep and later sleep-onset (Pereira, Semmer, & Elfering, 2014). Unnecessary tasks have also been associated with poorer mental health in general among 1351 Dutch employees over a 6-year follow-up period, and these effects have been more pronounced with those employees that had lower initial mental health (Madsen, Tripathi, Borritz, & Rugulies, 2014). As can be seen, illegitimate tasks have wide-ranging effects on employees' well-being, and this could also be a reason why illegitimate tasks affect ISB. When an employee is tired and stressed, one could be less willing to spend time in completing possibly time-consuming and inconvenient practices to ensure that their ISB is secure. The effect of technology-related stress has been previously studied in the context of ISP violation intentions, and it has been shown to increase the probability of violation intentions (D'Arcy et al., 2014). D'Arcy et al. (2014) also studied moral disengagement as a mediator between stress and intentions and noticed it be a significant mediator. One form of moral disengagement is shifting the blame to someone else, which is similar to the case of perceiving that someone else should do the tasks thought of as unnecessary. A similar notion of shifting the blame is also presented in a context of neutralization techniques that have been shown to predict ISB (Siponen & Vance, 2010).

However, these previous models (D'Arcy et al., 2014; Siponen & Vance, 2010) have not noticed the core process of the threat to self-esteem as a driving force in these evaluations. In summary, illegitimate tasks could affect ISB by causing additional stress to employees and increasing their experiences of being disrespected by their organization. When people experience that they are disrespected at work they tend to withdraw from being good organizational citizens (e.g., Semmer et al., 2010). A person could perceive that it is not reasonable to expect one to devote limited work time to learning ISP when one is already stressed out by other demands. The person could also experience that it is not part of one's job to take care of information security, but rather that it belongs to the information security professionals. Regarding more specific ISBs, for example, not transferring sensitive information to unsecured USB drive, could be perceived to be unreasonable if one is determined to take good care of the USB drive; demanding additional security measures could even be considered in a way that organization does not trust the employee in question.

Furthermore, the previous literature on information security behavior has not widely studied how perceiving ISP compliance as unnecessary determines how people act. It is possible that employees disobey the rules and regulations of an organization because they are seen as redundant. SOS explains how unnecessary tasks can be seen as threats to self and in this way lead to detrimental consequences for the organization. More specific security-related behaviors, such as locking the computer while leaving the workstation, could feel unnecessary if person evaluates that there is no risk of anyone using the open computer while one is away for a few minutes. In the context of different types of ISB, it could be that certain behaviors are considered to be more illegitimate than others and this way some behaviors could have a stronger association with illegitimacy evaluations while other behaviors are less affected by these evaluations.

SOS is expected to increase the understanding of the factors affecting ISB, and to add significant determinant of behavior to the more commonly used determinants, namely constructs from DT and PMT. Illegitimate tasks are expected to increase feelings of distress and insecurity and through to effect to one's self-image affect behavior (Semmer et al., 2007, 2015). Illegitimate tasks have been also empirically linked to counterproductive work behavior (e.g., Semmer et al., 2010; Stocker et al., 2010). SOS has not previously been used in the field of information security but in the present study unsecured ISB is contrasted to counterproductive work behavior and the following hypothesis can be formulated based on this notion. The general hypotheses could be tested separately regarding different behaviors to evaluate the generalizability of its association with ISB.

H12: Higher unnecessary tasks are negatively associated to secure ISB.
H13: Higher unreasonable tasks are negatively associated to secure ISB.

1.6 The Present Study

The aim of this study is to add new explanatory construct, namely illegitimate tasks from SOS, to understand ISB. This is applied together with more commonly used theoretical constructs from DT and PMT. Previous research on DT and PMT in the information security field have yielded mixed results (e.g., Cheng et al., 2013; Herath & Rao, 2009a; Vance et al., 2012) and it is possible that these discrepancies are due to context-specific differences in behavioral determinants. In addition to presenting new explanatory construct, this study investigates the roles of common and new determinants in explaining different ISBs. This approach will provide new information of the generalizability of the behavioral determinants and possibly illuminate the reasons for mixed results of previous research. The specific behaviors studied are not transferring confidential information to unsecured USB drives (USB), locking or logging out from the computer (LOG), and not writing down passwords (PSW) (adjusted from the list of the most common ISP violations, see Siponen & Vance, 2010). The present study also includes general ISP compliance as a behavior type since it has been used in many of the previous studies as a combination of different ISBs. The research model that functions as a starting point for this study is presented in Figure 1. It summarizes the theory-based general hypotheses.

The present study also includes control variables. Bernerth & Aguinis (2015) state that use of the control variables should be based on theory. PMT expects that people's previous experiences, knowledge, and expertise on the topic affect threat and coping appraisal processes (Floyd et al., 2000). In the context of information security behavior, information security knowledge could be an important factor affecting the behavior. There is also empirical evidence suggesting that security awareness affects appraisal processes which in turn affect security behavior (Hanus & Wu, 2016). On the basis of the importance of previous experiences and knowledge, general computer skills and work experience could also affect the behavior in the context of information security. Humaidi & Balakrishnan (2015) have shown that the determinants of information security compliance vary depending on the work experience of the employees. For these reasons information security knowledge, computer skills, and work experience are used as control variables in this study. In addition, age and gender are added as general control variables.

Research questions for this study are:

1) How do DT, PMT, and SOS explain different ISBs?
2) Are different constructs important in explaining different ISBs?

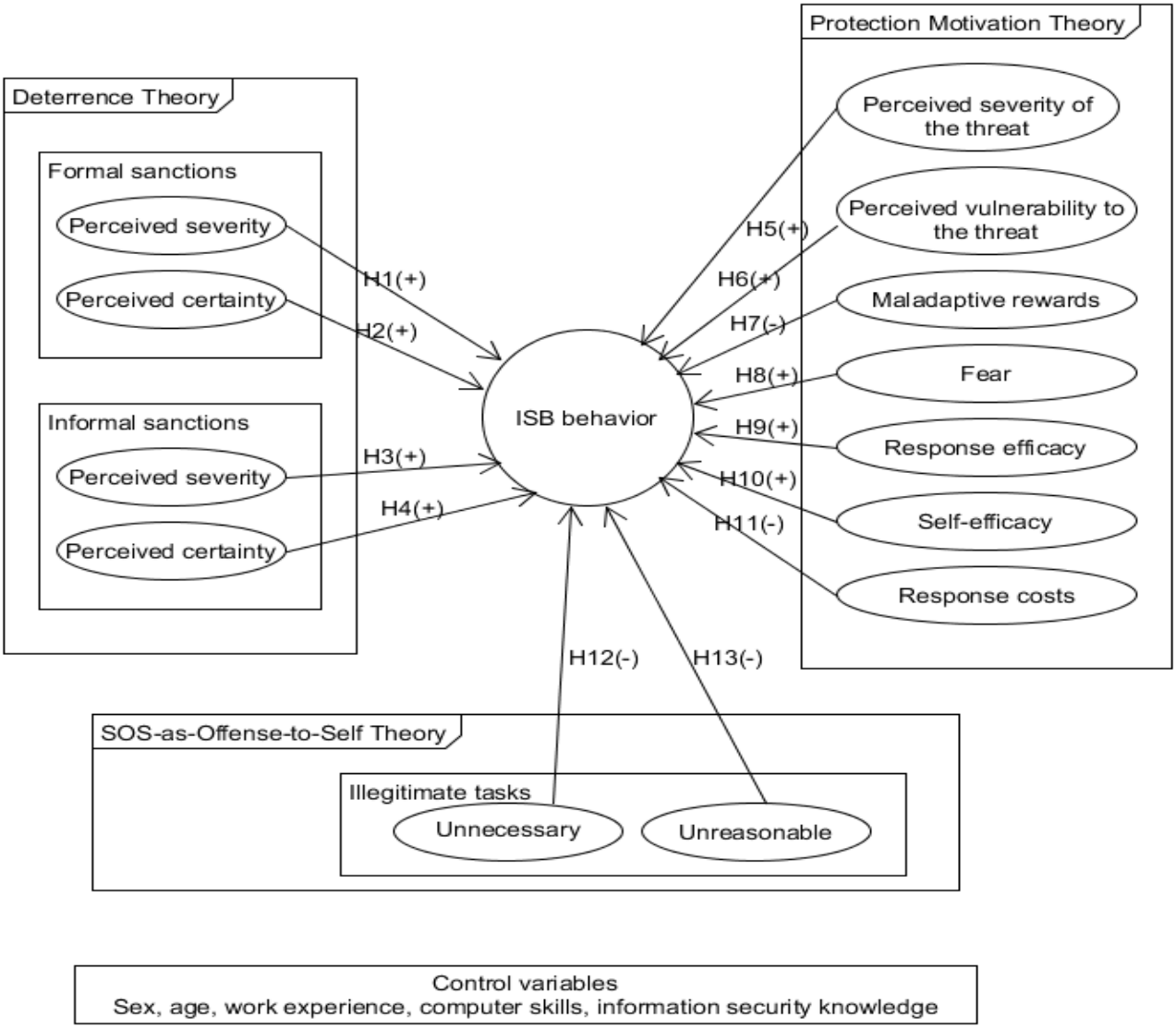

Figure 1 Research model

2 METHODS

2.1 Procedure and Participants

Participants were recruited from mass lectures at the university (n=83), from lunch cafeterias (n=141), from a public library (n=22), from the university lobby during the educational event (n=125), and from web forums (e.g., Facebook groups, Reddit) (n=89). They gave informed consent to participate in the study, and all the participants answered anonymously to one of the four behavior-specific questionnaires. There were 119 respondents to the ISP questionnaire, 111 to the USB questionnaire, 118 to the LOG questionnaire, and 112 to the PSW questionnaire. The four behavior-specific questionnaires were distributed randomly to the participants and the aim was to obtain behavior-specific samples that resemble each other in terms of background.

Background of the participants is shown in Table 1 which presents both behavior-specific and overall descriptive statistics. 55,5% of the participants were male, and 62,2% belonged to the age group of 20-30 years. Most of the participants (56,3%) had 1-7 years of work experience. Both computer skills and information security knowledge had relatively high means, indicating that the sample consisted of technologically savvy participants. The equality of means of background variables was tested across behaviors using one-way ANOVA with Tukey post-hoc tests. According to ANOVA results, there were no differences in sex, age, work experience, or computer skills between the behaviors. However, the behaviors differed in terms of information security knowledge (F[3]=21.56, p=.00). Respondents in ISP and PSW had less knowledge than participants in USB and LOG. Regarding these differences, it is important to take into account that knowledge items were behavior-specific and could not be readily comparable. Generally, the participants of the study resembled each other which improves the comparability of the behavioral determinants. Because the background of the participants is similar, possible differences between behavioral determinants are more likely due to the behaviors in question rather than to differences in sex, age, or other background factors. As an additional caution measure, background variables are added as controls to the analyses.

Table 1 Descriptive Statistics of the Participants

Descriptive	ISP (*n*=119)		USB (*n*=111)		LOG (*n*=118)		PSW (*n*=112)		Overall (*n*=460)	
	M(SD)	%	M(SD)	%	M(SD)	%	M(SD)	%	M(SD)	%
Sex	1.45(0.50)		1.50(0.50)		1.42(0.50)		1.46(0.50)		1.45(0.50)	
Male (1)		55.5		50.5		58.5		54.5		54.8
Female (2)		44.5		49.5		41.5		45.5		45.2
Age	2.73(1.13)		2.58(1.08)		2.58(1.07)		2.63(1.12)		2.63(1.10)	
Less than 20 years (1)		0.0		2.7		0.8		1.8		1.3
20-30 years (2)		62.2		64.0		69.5		65.2		65.2
31-40 years (3)		16.8		18.0		11.9		16.1		15.7
41-50 years (4)		10.9		7.2		7.6		6.3		8.0
51-60 years (5)		5.9		4.5		8.5		7.1		6.5
Over 60 years (6)		4.2		3.6		1.7		3.6		3.3
Work experience	2.64(1.14)		2.50(1.09)		2.42(1.11)		2.55(1.13)		2.53(1.12)	
Less than 1 year (1)		6.7		10.8		13.6		8.9		10.0
1-7 years (2)		56.3		54.1		56.8		57.1		56.1
8-15 years (3)		16.0		18.0		11.9		15.2		15.2
16-23 years (4)		8.4		8.1		9.3		7.1		8.3
Over 23 years (5)		12.6		9.0		8.5		11.6		10.4
Computer skills	4.11(0.80)		3.98(0.85)		3.94(0.79)		4.11(0.80)		4.03(0.81)	
Information security knowledge	4.73(1.71)		5.85(1.64)		6.04(1.25)		4.89(1.52)		5.37(0.08)	

Note. ISP = ISP compliance, USB = Not copying sensitive information to the unsecured USB drive, LOG = Locking or logging out from the computer, PSW = Not writing down passwords.
Numbers in the parentheses depict the value given to the respective category in the analyses.

2.2 Measures

The questionnaire used in the present study was formed based on previous questionnaires measuring similar theoretical constructs. It was focused on the ISB behavior in the work context and the respondents were instructed to answer to the questionnaire based on their experiences on their current job. If they were currently not working, they were asked to answer based on their experiences on their previous employment or work life in general. The questionnaire contained items related to four ISBs, DT, PMT, and SOS, as well as the background of the respondents. The items related to explanatory constructs were customized for each of the behaviors with as little alterations in meaning as possible. One person answered only one of the behavior-specific questionnaires. A scale ranging from 1 (completely disagree) – 7 (completely agree) was used for ISB and its determinants. These items were presented in random order. Used constructs and their items, as well as reliability and validity evaluation for the constructs are presented in section 2.2. Below is the general description of the origin of the items for each of the constructs.

Information security behaviors. Three of the four ISBs were selected based on the most common ISP security policy violations reported in Siponen and Vance (2010). Selected violations were reversed to represent secure ISB. The used ISBs were not copying sensitive data to the unsecured USB drive (USB), locking or logging out of the computer (LOG), and not writing down passwords (PSW). In addition, general ISP compliance (ISP) was included as one behavior since most of the previous studies have measured this as a dependent variable. The items were formulated based on behavior scenarios presented in Siponen and Vance (2010) and D'Arcy et al. (2014). When the questionnaire for USB was administered additional information was given to the respondents in the form of the following statement: In this questionnaire sensitive information refers to organization's information which is not public and which should not be given outside the organization without permission.

Deterrence Theory. Both formal (FS) and informal sanctions (IS) with evaluations for severity (S) and certainty (C) were included in the study. The items were formulated based on measures in Herath and Rao (2009b), Siponen et al. (2010), and Siponen & Vance (2010).

Protection Motivation Theory. Measures for threat severity (TSE) and vulnerability (TVU), maladaptive rewards (REW), fear (FEA), response efficacy (TRE), self-efficacy (SEF), and response costs (RCO) were included in the study. The items were formulated based on measures in Boss et al. (2015), Herath and Rao (2009b), and Siponen et al. (2010).

Stress-as-Offence-to-Self Theory. Illegitimate tasks (ITT) were measured using Bern Illegitimate Tasks Scale (BITS) (Semmer et al., 2010) as a basis for item formulation. Items for both unnecessary (IUN) and unreasonable (IUR) tasks were included. Compared to BITS, the items in the present study were modified to be statements instead of questions and the scale was the same 7-point Likert scale that was used with the other items in the present study.

Control variables. Measured background variables were sex, age, work experience, and computer skills (these were the same across the behaviors), and information security knowledge (behavior-specific items). Computer skills were measured by one-item evaluation of one's general computer skills, a scale ranging from 1 (Very poor skills) – 5 (Very good skills). Information security knowledge was measured by two items with a scale ranging

from 1 (completely disagree) – 7 (completely agree). The mean score of the two items was used in the analyses. Table 2 shows information security knowledge items and reliability statistics for their respective constructs.

Table 2 Information Security Knowledge Items and Their Reliability Statistics

Construct	α
ISP – Information security knowledge	.94
I know exactly what kinds of things the information security policy of my workplace includes.	
I am well informed of the information security policy of my workplace.	
USB – Information security knowledge	.78
I know that malware may transfer via USB drive.	
I understand that just sticking the USB drive to the computer may set off malware.	
LOG – Information security knowledge	.85
I understand all that can happen if someone gets access to a computer with my user identification.	
I understand precisely what can happen if someone gets access to a computer with my user identification.	
PSW – Information security knowledge	.45
I know how passwords are cracked.	
I understand what kinds of consequences are involved if a password is cracked.	

Note. α = Cronbach's alpha.

2.3 Validity and Reliability Assessment of the Measures

2.3.1 Assessment Methods

Before the beginning of data collection, preliminary validity and reliability assessment of the questionnaires was performed using two-phased pilot study. In the first phase, the questionnaires were presented at a university class where students answered to the questionnaire and gave informed consent to use the data. Following amounts of participants answered to the four questionnaires: 41 to ISP compliance (ISP), 35 to not copying sensitive information to the unsecured USB drive (USB), 38 to locking or logging out from the computer (LOG), and 34 to not writing down passwords (PSW). Since the sample sizes for each behavior-specific questionnaire were relatively small, CFA did not give reliable results for which reason Cronbach's alpha (α) was the method used for the assessment. Constructs with acceptable reliability were selected for the final questionnaire, and those with unacceptable statistics were reformulated and piloted again with a different group of students. Since the explanatory items from DT, PMT, and SOS were as similar as possible in wording, the second phase of piloting was completed with only ISP questionnaire. 20 participants answered to the questionnaire, and at this phase, almost all of the constructs had acceptable reliability statistics

and were selected for the final questionnaire. The few items of the constructs with poorer reliability were reformulated but not tested further.

All of the validity and reliability assessments were performed separately for the four ISBs with the actual data. There were 119 respondents to the general ISP compliance (ISP) questionnaire, 111 to the not copying sensitive data to the unsecured USB drive (USB) questionnaire, 118 to the locking or logging out of the computer (LOG) questionnaire, and 112 to the not writing down passwords (PSW) questionnaire. Content validity of the constructs was strengthened by using measurement items that had been tested in previous studies as a basis for the questionnaire formation. Convergent and discriminant validity were inspected using confirmatory factor analysis (CFA) with continuous factor indicators and maximum likelihood estimator (Muthén & Muthén, 1998-2012). CFA was selected because the constructs were based on strong theoretical foundation. Overall model fit was evaluated based on the following goodness-of-fit measures: Chi-Square (χ^2)-test, Root Mean Square Error of Approximation (RMSEA), Standardized Root Mean Square Residual (SRMR), Comparative Fit Index (CFI), and Tucker-Lewis Index (TLI) (Muthén & Muthén, 1998-2012; Schermelleh-Engel, Moosbrugger, & Müller, 2003).

Several theoretically plausible models were compared to find the empirically best-fitting model to be used in the further analyses. The sample size for each behavior was relatively small for CFA and in each of the behaviors, the number of parameters was larger than the sample size. CFAs were performed for overall models containing all the items and also separately for the items related to each of the three theories (i.e. DT, PMT, and SOS). By separate tests for the theories, the problems created by the small sample size could be mitigated and the overall model could be inspected in more detail. Original theory-based factors were combined in the tested models if the inter-construct correlations were high or if there were strong residual correlations between the items belonging to different factors. Theoretically plausible models (based on the expected direction of associations and previous studies combining the theoretical constructs) that differed from the original research model were also considered if the empirical data showed better fit for these models. The comparability of the four ISBs was also considered when choosing the model to be used in further analyses.

After testing the model fit, the items of each construct were inspected in more detail to further improve the overall model. Factor loadings for each item of the construct should exceed .70 and the average variance extracted (AVE) by the construct in each item should be greater than .50 to indicate good convergent validity and internal consistency of the measure (MacKenzie, Podsakoff, & Podsakoff, 2011; Fornell & Larcker, 1981). When there are problems with construct validity, elimination for problematic items is suggested to be done based on a) nonsignificant loadings on the hypothesized construct, b) squared standardized loadings that are less than .50, and c) significant and large measurement error covariances with other constructs (MacKenzie et al., 2011). Residuals were inspected in addition to loadings and error covariances to determine items to be deleted. Modification indices suggested by the program were utilized besides residuals in determining if items should be deleted or modifications allowed. Modifications were applied when they suggested significant residual intra-construct correlations and when the model improved by allowing these correlations. If modification indices suggested large inter-construct correlations the items in question were considered for deletion. After the final model was selected, the reliability of achieved constructs was assessed using Cronbach's alpha (α) where adequate interitem reliability is

achieved when α is greater than .70 (Nunnally & Bernstein, 1994). Overall, the complete models tested for each of the behaviors were:

1. Original research model: ISB and 4 constructs from DT, 7 from PMT, and 2 from SOS
2. Compressed model based on the theories: ISB and 2 constructs from DT (formal and informal sanctions), 3 constructs from PMT (threat and coping appraisal, as well as fear) and 1 from SOS (illegitimate tasks)
3. Theoretically plausible model based on separate CFAs for DT, PMT, and SOS: sanctions as a whole (DT), threat appraisal by threat severity and vulnerability, fear, combined maladaptive rewards and response costs, response efficacy, and self-efficacy (PMT), and illegitimate tasks as a whole (SOS)
4. The chosen model: Model 3 where problematic items have been removed and strong intra-construct correlations are allowed
5. Common method variance model: Model 4 where the constructs are loaded to first-order common method factor

Separate tests for each of the theories included:

6. DT: 4 constructs for severity and certainty of formal sanctions, as well as for severity and certainty of informal sanctions
7. DT: 2 constructs for formal and informal sanctions
8. DT: 1 construct for sanctions as a whole
9. DT: Model 7 where problematic items have been removed and strong intra-construct correlations are allowed
10. PMT: 7 constructs for threat severity and vulnerability, maladaptive rewards, fear, response efficacy, self-efficacy, and response costs
11. PMT: 3 factors for threat appraisal (threat severity and vulnerability, as well as maladaptive rewards), fear, and coping appraisal (response efficacy, self-efficacy, and response costs)
12. PMT: 5 constructs for threat appraisal (threat severity and vulnerability), maladaptive rewards, fear, coping appraisal (response efficacy and response costs), and self-efficacy
13. PMT: 4 constructs for combined threat and fear (threat severity and vulnerability, as well as fear), combined rewards and costs (maladaptive rewards and response costs), response efficacy, and self-efficacy
14. PMT: 5 constructs for threat appraisal (threat severity and vulnerability), combined rewards and costs (maladaptive rewards and response costs), fear, response efficacy, and self-efficacy
15. PMT: Model 14 where problematic items have been removed and strong intra-construct correlations are allowed

The factor solution for PMT was also tested in detail by separating parts of the overall model to determine the best-fitting model. For example, threat severity and vulnerability, as well as fear were tested separately to determine if they form a common factor or separate factors.

16. SOS: 2 constructs for unnecessary and unreasonable tasks

17. SOS: 1 construct for illegitimate tasks as a whole
18. SOS: Model 17 where problematic items have been removed and strong intra-construct correlations are allowed

In addition to assessing convergent validity and reliability of the constructs, discriminant validity was evaluated. These analyses are completed for the chosen model 4 for each of the ISBs. Discriminant validity is considered to be good if the square root of AVE for each construct is greater than all inter-construct correlations (Chin, 1998). In addition, effects of the common method bias were inspected. Common method bias refers to bias in the data created by certain response style of the respondents (Podsakoff, MacKenzie, & Podsakoff, 2012). Common method bias can affect construct validity and reliability, as well as bias the results of regression analyses. In the present study, common method bias is tested by adding a first-order method factor to the overall model. All of the constructs measured by the same questionnaire are loaded to this method factor, and then the loadings and explanatory levels of the common method factor are evaluated for the constructs (Podsakoff et al., 2012). CFAs were completed using Mplus version 7 (Muthén & Muthén, 1998-2012) and Cronbach's alphas were calculated using SPSS Statistics 22.

2.3.2 Assessment Results

Tables 3, 5, 7, and 9 shows the results of the model fits for each of the behaviors. The chosen model 4 did not have a perfect fit for any of the behaviors but the separate models for the constructs of DT, PMT, and SOS showed good or reasonable fit. Model 4 had also better fit than the other tested overall models for each of the behaviors. The poor overall fit could be due to small sample size compared to a number of free parameters in the models. The overall models were modified to fit the data as well as possible, and many of the original items were removed to improve the models. Fit indices showing the deviation from the fitting model (RMSEA, SRMR, CFI, and TLI) are close to the recommended cut-off scores after the modifications. The theoretical fit was also considered while testing the differing models, and Model 4 was the best compromise between empirical and theoretical expectations. With LOG, self-efficacy (SEF) was excluded because its items did not appear to form a unified construct nor did they correlate with other items in different constructs. The overall model was weaker with SEF. Tables 4, 6, 8, and 10 show that the factor loadings and item variance explained by the chosen constructs were high showing good convergent validity for all of the constructs. Reliability of the constructs was also acceptable as depicted in these tables.

However, there appeared to be problems with discriminant validity regarding all of the ISBs since the average square roots of AVE were not greater than the inter-construct correlations for all of the constructs, indicated in the comparison of the values in Tables 11-15. Square roots of AVE are presented in Table 11 and Tables 12-15 show inter-construct correlations for each of the ISBs. There were problems especially with the constructs for rewards and costs, as well as illegitimate tasks. In the case of PSW, the correlation between these constructs was over 1 indicating problems in the data. Although rewards and costs, as well as illegitimate tasks, appeared to be closely linked, they were not combined because they rep-

resented different theoretical foundations. In addition, analyses of common method bias indicate problems in the data. The overall models containing the common method factor (model 5) were not better overall fits than the chosen model 4 (shown in Tables 2, 4, 6, and 8) for any of the ISBs. However, Table 16 shows that the factor loadings and extracted variance of the constructs by the common method factor are considerably high for many of the constructs with each of the behaviors. Especially, the dependent variable ISB was highly explained by the common method factor in the cases of LOG and PSW. There were also problems with other constructs in terms of common method bias. The analysis of validity and reliability showed that although convergent validity appeared to be reasonable there were problems with discriminant validity and common method bias. These problems need to be taken into account when interpreting the results of the further analyses.

Table 3 ISP - Model fit indices for CFAs

Model	χ^2-test (df), *p*-value	RMSEA	SRMR	CFI	TLI
Cut-off score	*p*-value ≥.05	<.06	<.05	>.95	>.95
Overall models					
1	1439.284 (811), .0000	.081	.072	.798	.765
2	1928.686 (881), .0000	.100	.112	.664	.639
3	774.315 (496), .0000	.069	.064	.874	.858
4	523.189 (373), .0000	.058	.058	.916	.902
5	628.702 (393), .0000	.071	.115	.868	.854
Models for DT					
6	153.794 (48), .0000	.136	.066	.851	.795
7	175.602 (53), .0000	.139	.071	.828	.785
8	210.961 (54), .0000	.156	.075	.779	.730
9	23.828 (16), .0933	.064	.032	.982	.969
Models for PMT					
10	284.491 (168), .0000	.076	.064	.890	.862
11	667.912 (186), .0000	.148	.153	.545	.486
12	329.844 (179), .0000	.084	.083	.857	.833
13	430.169 (183), .0000	.107	.108	.766	.732
14	329.496 (179), .0000	.084	.073	.858	.833
15	237.133 (142), .0000	.075	.062	.893	.871
Models for SOS					
16	15.172 (19), .7116	.000	.033	1.000	1.027
17	15.307 (20), .7586	.000	.033	1.000	1.031
18	5.517 (13), .9620	.000	.022	1.000	1.061

Note. χ^2-test = Chi-Square test, df = degrees of freedom, RMSEA = Root Mean Square Error of Approximation, SRMR = Standardized Root Mean Square Residual, CFI = Comparative Fit Index, TLI = Tucker-Lewis Index.
The tested models are described on pages 26-27. For the chosen model 4, the following intra-construct correlations were allowed: FSC2 with FSS2, ISS3 with FSS1, ISC2 with ISS2, and REW3 with REW2.

Table 4 ISP - Constructs, Their Items, and Validity and Reliability Statistics

Construct	Items	F	V	α
ISP compliance (ISB)	1. I follow information security policy guidelines of my workplace.	.833	.693	.837
	2. I do not follow information security policy guidelines of my workplace. (R)	.794	.630	
	3. In my work, I act according to information security policy guidelines of my workplace.	.785	.616	
Sanctions (FIS)	1. I will be severely punished if I get caught of violating the company information security policy.	.666	.444	.925
	2. I will be subjected to disciplinary action if I get caught of violating the company information security policy.	.806	.649	
	3. I will be formally reprimanded if I get caught of violating the company information security policy.	*	*	
	4. I will probably be formally punished if I do not comply with the company information security policy.	*	*	
	5. I will probably be subjected to disciplinary action if I do not comply with the company information security policy.	.898	.806	
	6. I will eventually be formally punished if I do not comply with the company information security policy.	.759	.576	
	7. I will lose the trust of my manager if I get caught of violating the company information security policy.	*	*	
	8. I will lose my promotion prospects if management catches me of violating the company information security policy.	.762	.580	
	9. I will lose the respect of my manager if I get caught of violating the company information security policy.	.824	.679	
	10. It is probable that I will lose the trust of my manager if I do not comply with the company information security policy.	.720	.518	
	11. I will probably lose my promotion prospects if I do not comply with the company information security policy.	.784	.614	
	12. It is probable that I will lose the respect of my manager if I do not comply with the company information security policy.	*	*	
Threat appraisal (TAP)	1. A malicious security breach will follow the violation of information security policy.	.752	.566	.856
	2. If I do not comply with information security policy, it causes severe problems for my organization.	.765	.585	
	3. If I do not comply with the company information security policy, it will be followed by serious information security problems.	.855	.731	
	4. Being subjected to information security threat is probable if I do not comply with the company information security policy.	*	*	
	5. My company will be subjected to information security threat if I do not comply with the company information security policy.	.762	.581	
	6. Being subjected to information security threat is improbable even if I do not comply with the company information security policy. (R)	.560	.313	
Fear (FEA)	1. I am afraid of information security problems that will follow if I do not comply with the company information security policy.	.854	.729	.746
	2. I am anxious about information security problems that will follow if I do not comply with the company information security policy.	.697	.486	
	3. I am terrified by information security problems that will follow if I do not comply with the company information security policy.	*	*	

Rewards and costs (REC)	1. My work will slow down if I comply with the company information security policy.	*	*	.807
	2. Complying with the company information security policy reduces my productivity at work.	.572	.327	
	3. It makes my job easier if I do not comply with the company information security policy.	.660	.436	
	4. Complying with the company information security policy takes an unreasonable investment of effort.	.750	.562	
	5. There is too much work associated with complying with the company information security policy.	*	*	
	6. Complying with the company information security policy requires too much effort.	.769	.592	
Response efficacy (TRE)	1. Not complying with the information security policy increases the probability of information security threat realization.	.721	.519	.642
	2. Complying with the information security policy helps to avoid the realization of information security threat.	.657	.431	
	3. Careful compliance with information security policy decreases the probability of information security threat realization.	*	*	
Self-efficacy (SEF)	1. I can comply with the information security policy without help.	.742	.550	.782
	2. I can comply with the information security policy even if I would not receive help for it.	.868	.754	
	3. I can comply with the information security policy by myself.	*	*	
Illegitimate tasks (ITT)	1. I ponder if information security policy needs to be complied with at all.	*	*	.795
	2. I ponder if complying with information security policy makes sense at all.	.754	.568	
	3. I ponder if information security policy would need to be complied with if things were organized better.	.592	.350	
	4. I ponder if information security policy just exists because some people simply demand it this way.	*	*	
	5. I believe that someone else should take care of the realization of information security policy. *	*	*	
	6. Demand to comply unconditionally with the information security policy is going too far and should not be expected from me.	.745	.555	
	7. Demand to comply unconditionally with the information security policy puts me into an awkward position.	*	*	
	8. It is unfair for me to have to comply unconditionally with the information security policy.	.715	.511	

Note. R = Reversed scored, F = Factor loading for the respective construct, V = Variance explained by the respective construct, α = Cronbach's alpha, * = Removed from the model. Calculations for factor loadings and extracted variance are based on standardized model results.

Table 5 USB - Model fit indices for CFAs

Model	χ^2-test (df), *p*-value	RMSEA	SRMR	CFI	TLI
Cut-off score	*p*-value ≥.05	<.06	<.05	>.95	>.95
Overall models					
1	1447.117 (811), .0000	.084	.080	.811	.780
2	2056.743 (881), .0000	.110	.135	.651	.625
3	609.581 (404), .0000	.068	.065	.904	.889
4	460.443 (344), .0000	.055	.064	.939	.928
5	617.252 (364), .0000	.079	.140	.868	.853
Models for DT					
6	86.428 (48), .0006	.085	.040	.947	.927
7	98.178 (53), .0002	.088	.041	.938	.922
8	109.961 (54), .0000	.097	.046	.923	.905
9	27.451 (19), .0946	.063	.027	.980	.971
Models for PMT					
10	246.173 (168), .0001	.065	.063	.931	.914
11	737.692 (188), .0000	.162	.161	.514	.458
12	394.599 (179), .0000	.104	.137	.810	.777
13	330.728 (183), .0000	.085	.076	.869	.850
14	277.677 (179), .0000	.070	.068	.913	.898
15	96.297 (79), .0903	.044	.056	.976	.968
Models for SOS					
16	25.385 (19), .1483	.055	.064	.956	.934
17	33.867 (20), .0270	.079	.073	.903	.865
18	7.344 (5), .1963	.066	.043	.975	.949

Note. χ^2-test = Chi-Square test, df = degrees of freedom, RMSEA = Root Mean Square Error of Approximation, SRMR = Standardized Root Mean Square Residual, CFI = Comparative Fit Index, TLI = Tucker-Lewis Index.

The tested models are described on pages 26-27. For the chosen model 4, the following intra-construct correlations were allowed: FSC2 with FSS2, ISS3 with FSS1, ISS3 with FSC2, ISC2 with ISS2, and REW3 with REW1.

Table 6 USB - Constructs, Their Items, and Validity and Reliability Statistics

Construct	Items	F	V	α
Not copying sensitive information to the unsecured USB drive (ISB)	1. I sometimes put sensitive information on my computer to the unsecured USB drive. (R)	.798	.637	.840
	2. I sometimes transfer sensitive information related to my work to the unsecured USB drive. (R)	.863	.745	
	3. I have sensitive information related to my work on an unsecured USB drive. (R)	.701	.492	
Sanctions (FIS)	1. I will be severely punished if I get caught of transferring sensitive information to the unsecured USB drive.	.872	.761	.957
	2. I will be subjected to disciplinary action if I get caught of transferring sensitive information to the unsecured USB drive.	.855	.732	
	3. I will be formally reprimanded if I get caught of transferring sensitive information to the unsecured USB drive.	*	*	
	4. I will probably be formally punished if I transfer sensitive information to the unsecured USB drive.	*	*	
	5. I will probably be subjected to disciplinary action if I transfer sensitive information to the unsecured USB drive.	.863	.745	
	6. I will eventually be formally punished if I transfer sensitive information to the unsecured USB drive.	.870	.756	
	7. I will lose the trust of my manager if I get caught of transferring sensitive information to the unsecured USB drive.	*	*	
	8. I will lose my promotion prospects if management catches me of transferring sensitive information to the unsecured USB drive.	.744	.554	
	9. I will lose the respect of my manager if I get caught of transferring sensitive information to the unsecured USB drive.	.910	.828	
	10. It is probable that I will lose the trust of my manager if I transfer sensitive information to the unsecured USB drive.	*	*	
	11. I will probably lose my promotion prospects if I transfer sensitive information to the unsecured USB drive.	.856	.732	
	12. It is probable that I will lose the respect of my manager if I transfer sensitive information to the unsecured USB drive.	.857	.734	
Threat appraisal (TAP)	1. A malicious security breach will follow the transferring of sensitive information to the unsecured USB drive.	.860	.740	.858
	2. If I transfer sensitive information to the unsecured USB drive, it causes severe problems for my organization.	*	*	
	3. If I transfer sensitive information to the unsecured USB drive, it will be followed by serious information security problems.	.831	.691	
	4. Being subjected to information security threat is probable if I transfer sensitive information to the unsecured USB drive.	.623	.388	
	5. My company will be subjected to information security threat if I transfer sensitive information to the unsecured USB drive.	.815	.664	
	6. Being subjected to information security threat is improbable even if I transfer sensitive information to the unsecured USB drive. (R) *	*	*	
Fear (FEA)	1. I am afraid of information security problems that follow if I transfer sensitive information to the unsecured USB drive.	*	*	.846
	2. I am anxious about information security problems that follow if I transfer sensitive information to the unsecured USB drive.	.749	.561	
	3. I am terrified of information security problems that follow if I transfer sensitive information to the unsecured USB drive.	.978	.957	

Rewards and costs (REC)	1. My work will slow down if I do not transfer sensitive information to the unsecured USB drive.	.702	.492	.835
	2. Not transferring sensitive information to the unsecured USB drive reduces my productivity at work.	*	*	
	3. It makes my job easier if I transfer sensitive information to the unsecured USB drive.	.663	.439	
	7. Refraining from transferring sensitive information to the unsecured USB drive takes an unreasonable investment of effort.	*	*	
	8. There is too much work associated with taking care of information security by refraining from transferring sensitive information to the unsecured USB drive.	.836	.699	
	9. Refraining from transferring sensitive information to the unsecured USB drive requires too much effort.	.737	.543	
Response efficacy (TRE)	1. Transferring sensitive information to the unsecured USB drive increases the probability of information security threat realization.	.857	.734	.763
	2. Not transferring sensitive information to the unsecured USB drive helps to avoid the realization of information security threat.	.729	.532	
	3. Not transferring sensitive information to the unsecured USB drive decreases the probability of information security threat realization.	*	*	
Self-efficacy (SEF)	4. I can transfer sensitive information securely without help.	*	*	.941
	5. I can transfer sensitive information securely even if I would not receive help for it.	.975	.951	
	6. I can transfer sensitive information securely by myself.	.912	.831	
Illegitimate tasks (ITT)	1. I ponder if refraining from transferring sensitive information to the unsecured USB drive needs to be done at all. *	*	*	.732
	2. I ponder if refraining from transferring sensitive information to the unsecured USB drive makes sense at all.	.469	.220	
	3. I ponder if refraining from transferring sensitive information to the unsecured USB drive would need to be done if things were organized better. *	*	*	
	4. I ponder if transferring sensitive information to the unsecured USB drive just need to be refrained from because some people simply demand it this way.	.549	.302	
	5. I believe that someone else should take care of the security of transferring information to the USB drive. *	*	*	
	6. Demand to not to transfer sensitive information to the unsecured USB drive is going too far and should not be expected from me.	*	*	
	7. Demand to not to transfer sensitive information to the unsecured USB drive puts me into an awkward position.	.679	.461	
	8. It is unfair for me to have to refrain from transferring sensitive information to the unsecured USB drive.	.799	.638	

Note. R = Reversed scored, F = Factor loading for the respective construct, V = Variance explained by the respective construct, α = Cronbach's alpha, * = Removed from the model. Calculations for factor loadings and explained variance are based on standardized model results.

Table 7 LOG - Model fit indices for CFAs

Model	χ^2-test (df), *p*-value	RMSEA	SRMR	CFI	TLI
Cut-off score	*p*-value ≥.05	<.06	<.05	>.95	>.95
Overall models					
1	Nonidentified model				
2	1721.450 (881), .0000	.090	.122	.721	.700
3	687.767 (471), .0000	.062	.062	.905	.894
4	381.215 (301), .0012	.048	.054	.952	.944
5	480.570 (315), .0000	.067	.115	.900	.889
Models for DT					
6	95.822 (48), .0001	.092	.047	.916	.884
7	101.959 (53), .0001	.088	.049	.914	.892
8	101.016 (54), .0001	.086	.048	.917	.899
9	44.633 (34), .1049	.051	.035	.976	.969
Models for PMT					
10	268.612 (168), .0000	.071	.061	.901	.877
11	617.201 (186), .0000	.140	.161	.577	.522
12	383.495 (179), .0000	.098	.107	.799	.765
13	356.832 (183), .0000	.090	.070	.829	.804
14	291.642 (179), .0000	.073	.065	.890	.870
15	77.387 (69), .2287	.032	.046	.987	.983
Models for SOS					
16	11.175 (19), .9178	.000	.033	1.000	1.053
17	21.413 (20), .3732	.024	.044	.994	.991
18	12.376 (9), .1929	.057	.041	.979	.964

Note. χ^2-test = Chi-Square test, df = degrees of freedom, RMSEA = Root Mean Square Error of Approximation, SRMR = Standardized Root Mean Square Residual, CFI = Comparative Fit Index, TLI = Tucker-Lewis Index.

The tested models are described on pages 26-27. For the chosen model 4, the following intra-construct correlations were allowed: ISC2 with ISS2, and RCO2 with REW3. SEF is removed because it did not estimate properly.

Table 8 LOG - Constructs, Their Items, and Validity and Reliability Statistics

Construct	Items	F	V	α
Locking or logging out from computer (ISB)	1. I do not lock my computer when I leave my workstation for a short while. (R)	.672	.452	.801
	2. I do not always log out from my computer when I leave my work-station for a short while. (R)	.789	.623	
	3. I do not tend to lock or log out from the computer when I leave my workstation for a short while. (R)	.835	.697	

Sanctions (FIS)	1. I will be severely punished if I get caught of not locking or logging out from the computer when I leave my workstation for a short while.	.656	.431	.938
	2. I will be subjected to disciplinary action if I get caught of not locking or logging out from the computer when I leave my workstation for a short while.	.863	.744	
	3. I will be formally reprimanded if I get caught of not locking or logging out from the computer when I leave my workstation for a short while.	*	*	
	4. I will probably be formally punished if I do not lock or log out from the computer when I leave my workstation for a short while.	.756	.571	
	5. I will probably be subjected to disciplinary action if I do not lock or log out from the computer when I leave my workstation for a short while.	.876	.767	
	6. I will eventually be formally punished if I do not lock or log out from the computer when I leave my workstation for a short while.	*	*	
	7. I will lose the trust of my manager if I get caught of not locking or logging out from the computer when I leave my workstation for a short while.	*	*	
	8. I will lose my promotion prospects if management catches me of not locking or logging out from the computer when I leave my workstation for a short while.	.689	.474	
	9. I will lose the respect of my manager if I get caught of not locking or logging out from the computer when I leave my workstation for a short while.	.888	.789	
	10. It is probable that I will lose the trust of my manager if I do not lock or log out from the computer when I leave my workstation for a short while.	*	*	
	11. I will probably lose my promotion prospects if I do not lock or log out from the computer when I leave my workstation for a short while.	.781	.609	
	12. It is probable that I will lose the respect of my manager if I do not lock or log out from the computer when I leave my workstation for a short while.	.914	.836	
Threat appraisal (TAP)	1. A malicious security breach will follow not locking or logging out from the computer when I leave my workstation for a short while.	*	*	.785
	2. If I do not lock or log out from the computer when I leave my workstation for a short while, it causes severe problems for my organization.	.752	.566	
	3. If I do not lock or log out from the computer when I leave my workstation for a short while, it will be followed by serious information security problems.	.814	.614	
	4. Being subjected to information security threat is probable if I do not lock or log out from the computer when I leave my workstation for a short while.	.656	.430	
	5. My company will be subjected to information security threat if I do not lock or log out from the computer when I leave my workstation for a short while.	.586	.344	
	6. Being subjected to information security threat is improbable even if I do not lock or log out from the computer when I leave my workstation for a short while. (R) *	*	*	
Fear (FEA)	1. I am afraid of information security problems that will follow if I do not lock or log out from the computer when I leave my workstation for a short while.	.820	.672	.787
	2. I am anxious about information security problems that will follow if I do not lock or log out from the computer when I leave my workstation for a short while.	.793	.629	
	3. I am terrified by information security problems that will follow if I do not lock or log out from the computer when I leave my workstation for a short while.	*	*	

Rewards and costs (REC)	1. My work will slow down if I lock or log out from the computer when I leave my workstation for a short while.	.754	.569	.855
	2. Locking or logging out from the computer when I leave my workstation for a short while reduces my productivity at work.	*	*	
	3. It makes my job easier if I do not lock or log out from the computer when I leave my workstation for a short while.	.814	.663	
	4. Locking or logging out from the computer when I leave my workstation for a short while takes an unreasonable investment of effort.	.780	.608	
	5. There is too much work associated with taking care of information security by locking or logging out from the computer when I leave my workstation for a short while.	.800	.641	
	6. Locking or logging out from the computer when I leave my workstation for a short while requires too much effort.	*	*	
Response efficacy (TRE)	1. Not locking or logging out from the computer when I leave my workstation for a short while increases the probability of information security threat realization.	*	*	.759
	2. Locking or logging out from the computer when I leave my workstation for a short while helps to avoid the realization of information security threat.	.985	.970	
	3. Locking or logging out from the computer when I leave my workstation for a short while decreases the probability of information security threat realization.	.642	.413	
Self-efficacy (SEF)	4. I can lock and log out from the computer without help.	*	*	*
	5. I can lock and log out from the computer even if I would not receive help for it.	*	*	
	6. I can lock and log out from the computer by myself.	*	*	
Illegitimate tasks (ITT)	1. I ponder if locking or logging out from the computer always when leaving the workstation needs to be done at all.	*	*	.829
	2. I ponder if locking or logging out from the computer always when leaving the workstation makes sense at all.	.836	.700	
	3. I ponder if locking or logging out from the computer always when leaving the workstation would need to be done if things were organized better.	*	*	
	4. I ponder if locking or logging out from the computer always when leaving the workstation just need to be done because some people simply demand it this way.	.711	.505	
	5. I believe that someone else should take care of the computer security when I leave my workstation for a short while. *	*	*	
	6. Demand to lock or log out from the computer always when I leave my workstation for a short while is going too far and should not be expected from me.	.666	.444	
	7. Demand to lock or log out from the computer always when I leave my workstation for a short while puts me into an awkward position.	*	*	
	8. It is unfair for me to have to lock or log out from the computer always when I leave my workstation for a short while.	.751	.565	

Note. R = Reversed scored, F = Factor loading for the respective construct, V = Variance explained by the respective construct, α = Cronbach's alpha, * = Removed from the model. Calculations for factor loadings and explained variance are based on standardized model results.

Table 9 PSW - Model fit indices for CFAs

Model	χ^2-test (df), *p*-value	RMSEA	SRMR	CFI	TLI
Cut-off score	*p*-value ≥.05	<.06	<.05	>.95	>.95
Overall models					
1	1357.159 (811), .0000	.078	.069	.854	.830
2	1921.705 (881), .0000	.103	.134	.723	.702
3	815.099 (558), .0000	.064	.058	.915	.904
4	432.603 (345), .0009	.048	.048	.959	.952
5	606.059 (365), .0000	.077	.171	.887	.875
Models for DT					
6	114.133 (48), .0000	.111	.045	.897	.859
7	132.712 (53), .0000	.116	.048	.876	.846
8	139.684 (54), .0000	.119	.050	.867	.837
9	42.128 (32), .1086	.053	.024	.979	.970
Models for PMT					
10	238.181 (168), .0003	.061	.064	.937	.921
11	585.179 (186), .0000	.138	.173	.640	.593
12	402.709 (179), .0000	.106	.144	.798	.763
13	308.090 (183), .0000	.078	.074	.887	.870
14	267.464 (179), .0000	.066	.066	.920	.906
15	112.562 (120), .6726	.000	.049	1.000	1.010
Models for SOS					
16	29.568 (19), .0576	.070	.052	.964	.947
17	79.266 (20), .0000	.163	.075	.799	.718
18	2.826 (4), .5874	.000	.017	1.000	1.016

Note. χ^2-test = Chi-Square test, df = degrees of freedom, RMSEA = Root Mean Square Error of Approximation, SRMR = Standardized Root Mean Square Residual, CFI = Comparative Fit Index, TLI = Tucker-Lewis Index.

The tested models are described on pages 26-27. For the chosen model 4, the following intra-construct correlations were allowed: ISC3 with ISS2, REW2 with REW1, RCO3 with RCO1, and IUN2 with IUN1.

Table 10 PSW - Constructs, Their Items, and Validity and Reliability Statistics

Construct	Items	F	V	α
Not writing down passwords (ISB)	1. I put down my passwords for recalling. (R)	.942	.887	.930
	2. I write down my passwords. (R)	.923	.852	
	3. I write down my passwords to remember it. (R)	*	*	
Sanctions (FIS)	1. I will be severely punished if I get caught of writing my password down.	*	*	.948
	2. I will be subjected to disciplinary action if I get caught of writing my password down.	.904	.817	
	3. I will be formally reprimanded if I get caught of writing my password down.	.853	.728	
	4. I will probably be formally punished if I write my password down.	.766	.587	
	5. I will probably be subjected to disciplinary action if I write my password down.	*	*	
	6. I will eventually be formally punished if I write my password down.	.937	.878	
	7. I will lose the trust of my manager if I get caught of writing my password down.	*	*	
	8. I will lose my promotion prospects if management catches me of writing my password down.	.796	.633	
	9. I will lose the respect of my manager if I get caught of writing my password down.	.922	.849	
	10. It is probable that I will lose the trust of my manager if I write my password down.	.784	.614	
	11. I will probably lose my promotion prospects if I write my password down.	*	*	
	12. It is probable that I will lose the respect of my manager if I write my password down.	.899	.808	
Threat appraisal (TAP)	1. A malicious security breach will follow writing down the password.	*	*	.892
	2. If I write my password down, it causes severe problems for my organization.	.837	.701	
	3. If I write my password down, it will be followed by serious information security problems.	.864	.747	
	4. Being subjected to information security threat is probable if I write my password down.	.743	.552	
	5. My company will be subjected to information security threat if I write my password down.	.847	.717	
	6. Being subjected to information security threat is improbable even if I write my password down. (R) *	*	*	
Fear (FEA)	1. I am afraid of information security problems that will follow if I write my password down.	.690	.477	.816
	2. I am anxious about information security problems that will follow if I write my password down.	.809	.654	
	3. I am terrified by information security problems that will follow if I write my password down.	.839	.704	

Rewards and costs (REC)	1. My work will slow down if I do not write my password down.	.716	.513	.847
	2. Refraining from writing down the password reduces my productivity at work.	.553	.306	
	3. It makes my job easier if I write my password down.	*	*	
	4. Memorizing the passwords takes an unreasonable investment of effort.	.784	.615	
	5. There is too much work associated with memorizing the passwords.	*	*	
	6. Memorizing the passwords requires too much effort.	.824	.679	
Response efficacy (TRE)	1. Writing down the password increases the probability of information security threat realization.	*	*	.820
	2. Refraining from writing down the password helps to avoid the realization of information security threat.	.809	.761	
	3. Refraining from writing down the password decreases the probability of information security threat realization.	.797	.636	
Self-efficacy (SEF)	1. I can remember my passwords without help.	.850	.722	.704
	2. I can remember my passwords even if I would not receive help for it.	*	*	
	3. I have my passwords memorized.	.778	.606	
Illegitimate tasks (ITT)	1. I ponder if all the passwords need to be memorized at all.	.452	.204	.835
	2. I ponder if memorizing all the passwords makes sense at all.	.677	.458	
	3. I ponder if all the passwords need to be memorized if things were organized better. *	*	*	
	4. I ponder if memorizing all the passwords is just demanded because some people simply demand it this way. *	*	*	
	5. I believe that someone else should take care of the password security. *	*	*	
	6. Demand to memorize all the passwords is going too far and should not be expected from me.	.924	.854	
	7. Demand to memorize all the passwords puts me into an awkward position.	*	*	
	8. It is unfair for me to have to memorize all the passwords.	.808	.653	

Note. R = Reversed scored, F = Factor loading for the respective construct, V = Variance explained by the respective construct, α = Cronbach's alpha, * = Removed from the model. Calculations for factor loadings and extracted variance are based on standardized model results.

Table 11 Constructs, Their Average Variance Extracted (AVE), and Square Root of AVE

Construct	AVE	$\sqrt{AVE}$	Construct	AVE	$\sqrt{AVE}$
ISP.ISB	.646	.804	**LOG.ISB**	.591	.769
ISP.FIS	.608	.780	**LOG.FIS**	.653	.808
ISP.TAP	.555	.745	**LOG.TAP**	.489	.699
ISP.FEA	.608	.780	**LOG.FEA**	.651	.807
ISP.REC	.479	.692	**LOG.REC**	.620	.787
ISP.TRE	.475	.689	**LOG.TRE**	.692	.832
ISP.SEF	.652	.808	**LOG.SEF**	-	-
ISP.ITT	.496	.704	**LOG.ITT**	.554	.744
USB.ISB	.625	.791	**PSW.ISB**	.870	.933
USB.FIS	.730	.854	**PSW.FIS**	.739	.860
USB.TAP	.621	.788	**PSW.TAP**	.679	.824
USB.FEA	.759	.871	**PSW.FEA**	.612	.782
USB.REC	.543	.737	**PSW.REC**	.528	.727
USB.TRE	.633	.796	**PSW.TRE**	.699	.836
USB.SEF	.891	.944	**PSW.SEF**	.664	.815
USB.ITT	.405	.636	**PSW.ITT**	.542	.736

Note. AVE = Average variance extracted by the construct; calculated as a mean of the variance explained by the construct for each item in it. The abbreviations are the same as presented in Tables 3, 5, 7, and 9.
Values are presented for the chosen model 4. Calculations are based on standardized model results.

Table 12 ISP - Correlations between the Constructs

Construct	1	2	3	4	5	6	7
1 ISB	-						
2 FIS	.134						
3 TAP	.434**	.554**					
4 FEA	.179	.295*	.513**				
5 REC	-.679**	.045	-.368**	.114			
6 TRE	.709**	.207	.616**	.281*	-.484**		
7 SEF	.386**	-.125	-.033	-.350**	-.295**	.080	
8 ITT	-.818**	-.228*	-.583**	-.295**	.856**	-.810**	-.272*

Note. The abbreviations are the same as presented in Table 3.
Calculations are based on standardized model results.
* p < .05, ** p < .01.

Table 13 USB - Correlations between the Constructs

Construct	1	2	3	4	5	6	7
1 ISB	-						
2 FIS	.231						
3 TAP	.259*	.759**					
4 FEA	.169	.542**	.653**				
5 REC	-.744**	-.244*	-.282**	-.108			
6 TRE	.154	.488**	.840**	.320**	-.343**		
7 SEF	.017	-.039	.226*	-.066	-.281*	.289*	
8 ITT	-.571**	-.061	-.226	.005	.904**	-.405**	-.261*

Note. The abbreviations are the same as presented in Table 5.
Calculations are based on standardized model results.
* p < .05, ** p < .01.

Table 14 LOG - Correlations between the Constructs

Construct	1	2	3	4	5	6
1 ISB	-					
2 FIS	.195					
3 TAP	.556**	.553**				
4 FEA	.569**	.416**	.745**			
5 REC	-.711**	.069	-.191	-.167		
6 TRE	.464**	.062	.406**	.304**	-.296**	
7 ITT	-.773**	-.114	-.293*	-.211	.765**	-.397**

Note. The abbreviations are the same as presented in Table 7.
Calculations are based on standardized model results.
* p < .05, ** p < .01.

Table 15 PSW - Correlations between the Constructs

Construct	1	2	3	4	5	6	7
1 ISB	-						
2 FIS	.270**						
3 TAP	.427**	.659**					
4 FEA	.073	.553**	.754**				
5 REC	-.794**	-.250*	-.303**	.001			
6 TRE	.433**	.330**	.655**	.496**	-.332**		
7 SEF	.663**	.271**	.419**	.208	-.720**	.491**	
8 ITT	-.754**	-.215*	-.322**	-.100	1.010**	-.432**	-.709**

Note. The abbreviations are the same as presented in Table 9.
Calculations are based on standardized model results.
* p < .05, ** p < .01.

Table 16 Study Contructs - Factor Loadings and Extracted Variance by the Common Method Factor

Construct	F	V	Construct	F	V
ISP.ISB	.807	.349	**LOG.ISB**	.982	.965
ISP.FIS	.215	.954	**LOG.FIS**	.231	.053
ISP.TAP	.570	.675	**LOG.TAP**	.544	.296
ISP.FEA	.192	.963	**LOG.FEA**	.506	.256
ISP.REC	-.795	.368	**LOG.REC**	-.723	.523
ISP.TRE	.791	.374	**LOG.TRE**	.446	.199
ISP.SEF	.249	.938	**LOG.SEF**	-	-
ISP.ITT	-1.040	-.082	**LOG.ITT**	-.802	.643
USB.ISB	.232	.054	**PSW.ISB**	.798	.636
USB.FIS	.708	.501	**PSW.FIS**	.286	.082
USB.TAP	1.078	Undefined	**PSW.TAP**	.406	.165
USB.FEA	.622	.387	**PSW.FEA**	.131	Undefined
USB.REC	-.263	.069	**PSW.REC**	-1.004	.017
USB.TRE	.783	.613	**PSW.TRE**	.456	.208
USB.SEF	.201	.040	**PSW.SEF**	.750	.562
USB.ITT	-.199	.040	**PSW.ITT**	-.977	.954

Note. F = Factor loading for the common method factor, V = Variance explained by the common method factor. The abbreviations are the same as presented in Tables 3, 5, 7, and 9. Calculations for factor loadings and extracted variance are based on standardized model results in model 5 presented on page 26 for each of the ISBs.

2.4 Analysis Strategy

Based on the reliability and validity assessment, the final hypotheses tested in this study were:

H1: Higher sanctions are positively associated to secure ISB.
H2: Higher threat appraisal is positively associated to secure ISB.
H3: Higher fear is positively associated to secure ISB.
H4: Higher rewards and costs are negatively associated to secure ISB.
H5: Higher response efficacy is positively associated to secure ISB.
H6: Higher self-efficacy is positively associated to secure ISB.
H7: Higher amount of illegitimate tasks is negatively associated to secure ISB.

A regression model was used to answer research questions. Gefen, Straub, and Boudreau (2000) have suggested guidelines for IS researches of when to use structural equation modeling (SEM) compared to more traditional regression techniques. Although SEM is considered to be the state-of-the-art approach, there are situations when regression analysis could be more appropriate, such as smaller sample size and problems with distribution and multicollinearity assumptions. The results of regression analysis tend to be robust even when the assumptions are not fully met. In the present sample, the sample sizes for each behavior-specific questionnaire (n=112-119) were relatively small compared to the amount of explanatory factors (i.e. independent variables). The observed variables also correlated relatively

highly with each other suggesting possible problems with multicollinearity. For these reasons, linear regression analysis was chosen as the analysis strategy. Data sets were almost complete; missing data was due to a few participants that discontinued answering to the questionnaire.

Hierarchical linear regression analysis was completed separately for each ISB. In the first step, only the control variables were put into the model, and in the second step, the study constructs were added. This way it could be evaluated if the study constructs predict ISBs above and beyond the effect of controls. Since the aim was to investigate how the theoretical constructs from DT, PMT, and SOS explain ISBs, the used model was forced. The significance of the study constructs was evaluated by comparing explanatory levels i.e. R^2 values of Model 1 (including only the control variables) and Model 2 (including the controls and the study constructs). F-test was completed for R^2 values to inspect the statistical significance of the difference between the models. A p-value < .05 for F-test indicate that the change in R^2 is significant and the study variables add explanatory value over the controls. Standardized estimates (β) for regression coefficients of the constructs were also calculated and evaluated by t-test. If p-value < .05 for t-test, it indicates that the construct is a reliable explanatory factor.

To evaluate the results of the analyses, assumptions of the regression analysis were inspected. The chosen constructs need to be meaningful explanatory factors for the dependent variable which is partly indicated by the correlations between the constructs (Metsämuuronen, 2005). Tables 11-15 show that for each ISB, there were significant correlations between ISB and explanatory constructs which indicated that the constructs are relevant. Green (1991) suggests that in regression techniques accurate sample size is $N > 50 + 8$ x the amount of independent variables for the multiple correlation and $N > 104 +$ a number of independent variables for the partial correlation. When both are tested, the larger sample size should be selected. In the present study, these numbers were 114 and 112 which made the sample sizes for each behavior adequate for the analyses. It is also expected that there are not outliers that deviate too far from the sample mean of each construct. Observations that were more than three standard deviations from the sample mean were relocated to the tails (3 SD) of the distribution of the variable before the analyses.

In addition, it is expected that there is no multicollinearity between the explanatory constructs (i.e. they do not correlate too strongly with each other) and residuals should be normally distributed and homoscedastic (i.e. the variance is homogenous) (Metsämuuronen, 2005). Multicollinearity was tested by tolerance values and variance inflation factors (VIF). Low tolerance values, especially when near zero, and high VIF values indicate problems in the data. Eigenvalues, condition index, and variance proportions are evaluated to check for multicollinearity. Eigenvalues near zero, condition index over 15, and if there are large variance proportions together with high condition index, indicate that multicollinearity is a problem in the data (Metsämuuronen, 2005). Studentized deleted residuals were used for the residual investigation. The normality of the residuals was investigated by checking normal probability plots. If the residuals are on a straight line, it indicates that they are normally distributed. Homoscedasticity of the residuals was inspected by looking at the figures showing residuals and predicted values at the same time with residuals and individual observations for the constructs. By the distribution of the observations in the figures, the homoscedasticity of the residuals can be evaluated. Results of residual inspection and multicollinearity diagnostics are reported in the results section. IBM SPSS Statistics 22 were used for the regression analyses.

3 RESULTS

3.1 Determinants of ISP

Model 1 with only the control variables was compared with Model 2 that included the study constructs in addition to the controls. Results of the regression analysis for ISP are presented in Table 17. Model 2 added explanatory power to Model 1 indicating that the constructs from DT, PMT, and SOS predicted general information security policy compliance (ISP) above and beyond of control variables. Model 2 explained 53% of the variance in ISP of which 35.5% were due to the addition of the study constructs. Significant predictors of ISP included response efficacy, self-efficacy, and illegitimate tasks of which illegitimate tasks was negatively, and response efficacy and self-efficacy were positively associated to ISP. Regression coefficient was highest for illegitimate tasks indicating that they affected the most strongly to ISP. However, the difference in coefficients between the significant coefficients was relatively small. Based on the results, people tend to follow ISP when they feel that their actions have an effect on the overall information security of their workplace and when they evaluate themselves to be capable of following ISP. When people experience the following the ISP to be unreasonable for their role or unnecessary altogether, they are less inclined to comply with ISP. Of the general hypotheses, H5-H7 were supported and H1-H4 were not in the case of ISP.

Based on the residual figures, the residuals were reasonably well normally distributed and homoscedastic. However, there were potential problems with multicollinearity in Model 2, indicated by part of the multicollinearity statistics. Tolerance values varied between .213 and .756 and VIF values between 1.324 and 4.699. REC, TRE, SEF, and ITT all had small eigenvalues (.003-.028) and high condition indexes (20.412-61.566). Variance proportions were relatively low. Possible problems with multicollinearity were expected already based on the analyses of discriminant validity and common method bias. All of the significant predictors had problems with multicollinearity, so the results regarding their importance need to be interpreted with caution.

Table 17 ISP - Results of the Hierarchical Regression Analysis

Overall Model Results					
Model	**R^2**	**R^2 change**	**F change**	**df1, df2**	**Sig. F change**
Model 1	.175	.175	4.791	5, 113	.001
Model 2	.530	.355	11.455	7, 106	.000
Regression Coefficients for Model 2					
Construct	**β**	**t-test**	**Sig. t-test**	**TOL**	**VIF**
Constant		4.027	.000		
Sex	.014	.176	.860	.756	1.324
Age	-.008	-.055	.956	.217	4.611
Work experience	.083	.573	.568	.213	4.699
Computer skills	-.013	-.169	.866	.760	1.316
Information security knowledge	.131	1.705	.091	.755	1.325
Sanctions (FIS)	.038	.478	.633	.699	1.430
Threat appraisal (TAP)	-.006	-.063	.950	.479	2.087
Fear (FEA)	.108	1.257	.212	.601	1.664
Rewards and costs (REC)	-.181	-1.861	.065	.468	2.136
Response efficacy (TRE)	.241	2.871	.005	.629	1.589
Self-efficacy (SEF)	.210	2.595	.011	.677	1.477
Illegitimate tasks (ITT)	-.281	-2.523	.013	.357	2.799

Note. R^2 = Explanatory level of the model, F change = F-test for the change in explanatory level, df = degrees of freedom, Sig. F change = *p*-value for F-test, β = standardized regression coefficient estimate, Sig. t-test = *p*-value for t-test, TOL = Tolerance, VIF = Variance inflation factor.

3.2 Determinants of USB

Model 1 with only the control variables was compared with Model 2 that included the study constructs in addition to the controls. Results of the regression analysis for USB are presented in Table 18. Model 2 added explanatory power to Model 1 indicating that the constructs from DT, PMT, and SOS predicted not copying sensitive information to the unsecured USB drive (USB) above and beyond of control variables. Model 1 was not statistically significant which strengthened the significance of study constructs as predictors of USB. Model 2 explained 51.1% of the variance in USB of which 48.3% were due to the addition of the study constructs. Significant predictors of USB included work experience, threat appraisal, as well as rewards and costs. Threat appraisal was positively, and work experience and rewards and costs were negatively associated to USB. Regression coefficient was highest for rewards and costs indicating that they affected the most strongly to USB. Based on these results, people tend to use USB drives securely when they feel threatened by the consequences of not doing so. However, if people evaluate that they benefit of not acting securely, they tend to ignore fears related to

unsecured USB use. Of the general hypotheses, H2 and H4 were supported but other hypotheses were not in the case of USB. In addition, work experience appeared to affect people's actions regarding USB use in a way that more experienced employees are less inclined to withheld from copying sensitive information to unsecured USB drive.

Based on the residual figures, the residuals were reasonably well normally distributed and homoscedastic. However, there were potential problems with multicollinearity in Model 2, indicated by part of the multicollinearity statistics. Tolerance values varied between .260 and .760 and VIF values between 1.316 and 3.900. FEA, REC, TRE, SEF, and ITT all had small eigenvalues (.006-.040) and high condition indexes (17.111-45.787). Variance proportions were relatively low. Possible problems with multicollinearity were expected already based on the analyses of discriminant validity and common method bias. Of the significant predictors, rewards and costs had problems with multicollinearity, so the results regarding their importance need to be interpreted with caution.

Table 18 USB - Results of the Hierarchical Regression Analysis

Overall Model Results					
Model	**R^2**	**R^2 change**	**F change**	**df1, df2**	**Sig. F change**
Model 1	.027	.027	.579	5, 103	.716
Model 2	.511	.483	13.547	7, 96	.000
Regression Coefficients for Model 2					
Construct	**β**	**t-test**	**Sig. t-test**	**TOL**	**VIF**
Constant		6.456	.000		
Sex	-.034	-.420	.675	.760	1.316
Age	.234	1.676	.097	.261	3.827
Work experience	-.281	-2.008	.047	.260	3.851
Computer skills	-.140	-1.437	.154	.535	1.867
Information security knowledge	.069	.813	.418	.706	1.416
Sanctions (FIS)	-.056	-.524	.602	.447	2.238
Threat appraisal (TAP)	.288	2.041	.044	.256	3.900
Fear (FEA)	-.111	-1.166	.246	.567	1.764
Rewards and costs (REC)	-.665	-6.235	.000	.448	2.230
Response efficacy (TRE)	-.162	-1.510	.134	.441	2.270
Self-efficacy (SEF)	-.068	-.738	.462	.602	1.662
Illegitimate tasks (ITT)	-.083	-.735	.464	.401	2.495

Note. R^2 = Explanatory level of the model, F change = F-test for the change in explanatory level, df = degrees of freedom, Sig. F change = *p*-value for F-test, β = standardized regression coefficient estimate, Sig. t-test = *p*-value for t-test, TOL = Tolerance, VIF = Variance inflation factor.

3.3 Determinants of LOG

Model 1 with only the control variables was compared with Model 2 that included the study constructs in addition to the controls. Results of the regression analysis for LOG are presented in Table 19. Model 2 added explanatory power to Model 1 indicating that the constructs from DT, PMT, and SOS predicted locking or logging out from the computer (LOG) above and beyond of control variables. Model 1 was not statistically significant which strengthened the significance of study constructs as predictors of LOG. Model 2 explained 56.3% of the variance in LOG of which 54.4% were due to the addition of the study constructs. Significant predictors of LOG included fear, rewards and costs, as well as illegitimate tasks. Fear was positively, and illegitimate tasks and rewards and costs were negatively associated to LOG. Regression coefficient was highest for illegitimate tasks indicating that they affected the most strongly to ISP. However, the difference in coefficients between the significant coefficients was relatively small. Based on these results, people tend to lock or log out from the computer when they fear the consequences of not doing so. However, if people evaluate that they benefit of not acting securely or if they experience LOG procedures to be unreasonable or unnecessary, they are more likely to left the computer unlocked while leaving the workstation for a short while. Of the general hypotheses, H3, H4 and H7 were supported but other hypotheses were not in the case of LOG.

Based on the residual figures, the residuals were reasonably well normally distributed and homoscedastic. However, there were potential problems with multicollinearity in Model 2, indicated by part of the multicollinearity statistics. Tolerance values varied between .179 and .742 and VIF values between 1.190 and 5.594. REC, TRE, and ITT all had small eigenvalues (.007-.025) and high condition indexes (20.514-38.071). Variance proportions were relatively low. Possible problems with multicollinearity were expected already based on the analyses of discriminant validity and common method bias. Of the significant predictors, rewards and costs, as well as illegitimate tasks had problems with multicollinearity, so the results regarding their importance need to be interpreted with caution.

Table 19 LOG - Results of the Hierarchical Regression Analysis

Overall Model Results					
Model	**R^2**	**R^2 change**	**F change**	**df1, df2**	**Sig. F change**
Model 1	.061	.061	1.421	5, 110	.222
Model 2	.563	.544	23.837	6, 104	.000
Regression Coefficients for Model 2					
Construct	**β**	**t-test**	**Sig. t-test**	**TOL**	**VIF**
Constant		2.745	.007		
Sex	-.075	-1.051	.296	.742	1.348
Age	.052	.362	.718	.186	5.382
Work experience	.022	.154	.878	.179	5.594
Computer skills	.046	.640	.524	.724	1.380
Information security knowledge	.050	.743	.459	.840	1.190
Sanctions (FIS)	-.063	-.834	.406	.675	1.481
Threat appraisal (TAP)	.133	1.497	.137	.484	2.064
Fear (FEA)	.301	3.760	.000	.592	1.690
Rewards and costs (REC)	-.270	-3.206	.002	.538	1.860
Response efficacy (TRE)	.052	.738	.462	.771	1.298
Illegitimate tasks (ITT)	-.355	-4.112	.000	.510	1.959

Note. R^2 = Explanatory level of the model, F change = F-test for the change in explanatory level, df = degrees of freedom, Sig. F change = *p*-value for F-test, β = standardized regression coefficient estimate, Sig. t-test = *p*-value for t-test, TOL = Tolerance, VIF = Variance inflation factor.

3.4 Determinants of PSW

Model 1 with only the control variables was compared with Model 2 that included the study constructs in addition to the controls. Results of the regression analysis for PSW are presented in Table 20. Model 2 added explanatory power to Model 1 indicating that the constructs from DT, PMT, and SOS predicted not writing down passwords (PSW) above and beyond of control variables. Model 2 explained 57.9% of the variance in PSW of which 41.3% were due to the addition of the study constructs. Rewards and costs were the only significant predictor of PSW, and it was negatively associated to PSW. Based on these results, people are likely to write down their passwords if they experience that they gain something or save resources by doing that. Of the general hypotheses, only H4 was supported in the case of PSW.

Based on the residual figures, the residuals were reasonably well normally distributed and homoscedastic. However, there were potential problems with multicollinearity in Model 2, indicated by part of the multicollinearity statistics. Tolerance values varied between .153 and .737 and VIF values between 1.358 and 6.516. FEA, REC, TRE, SEF, and ITT all had small eigenvalues (.007-.043) and high condition indexes (16.240-40.515). Variance proportions were relatively low. Possible problems with multicollinearity were expected already based

on the analyses of discriminant validity and common method bias. The only significant predictor, rewards and costs, had problems with multicollinearity, so the results regarding its importance need to be interpreted with caution. Problems with the data could also affect the other predictors being non-significant by t-test estimation.

Table 20 PSW - Results of the Hierarchical Regression Analysis

Overall Model Results					
Model	**R^2**	**R^2 change**	**F change**	**df1, df2**	**Sig. F change**
Model 1	.166	.166	4.211	5, 106	.002
Model 2	.579	.413	13.868	7, 99	.000
Regression Coefficients for Model 2					
Construct	**β**	**t-test**	**Sig. t-test**	**TOL**	**VIF**
Constant		4.488	.000		
Sex	-.081	-1.029	.306	.690	1.450
Age	-.098	-.586	.559	.153	6.516
Work experience	.052	.325	.746	.163	6.137
Computer skills	-.072	-.946	.347	.737	1.358
Information security knowledge	.016	.191	.849	.639	1.565
Sanctions (FIS)	.020	.228	.820	.543	1.840
Threat appraisal (TAP)	.224	1.923	.057	.313	3.191
Fear (FEA)	-.149	-1.531	.129	.449	2.227
Rewards and costs (REC)	-.333	-2.955	.004	.336	2.978
Response efficacy (TRE)	.085	.997	.321	.585	1.709
Self-efficacy (SEF)	.158	1.758	.082	.525	1.906
Illegitimate tasks (ITT)	-.194	-1.732	.086	.340	2.941

Note. R^2 = Explanatory level of the model, F change = F-test for the change in explanatory level, df = degrees of freedom, Sig. F change = *p*-value for F-test, β = standardized regression coefficient estimate, Sig. t-test = *p*-value for t-test, TOL = Tolerance, VIF = Variance inflation factor.

3.5 Comparing the Determinants of ISBs

Comparison of the main regression results is presented in Figure 1. The overall explanatory level for the behavior varied between 51.1-57.9%, which shows that together the control variables and the constructs of DT, PMT, and SOS explained over half of the variance in different ISBs. PSW had the highest overall explanatory level, although only one of its determinants was in itself significant predictor of behavior. Illegitimate tasks were the strongest determinant of both ISP and LOG, but the difference between it and other significant predictors was not large. ISP and LOG differed on the other significant determinants in a way that general ISP compliance was predicted by response efficacy and self-efficacy while locking or logging out from the computer was predicted by fear, as well as rewards and costs. Secure USB use was in turn predicted by threat appraisal, rather than fear itself. In the case of USB, rewards

and costs were a considerably stronger determinant of behavior than the other significant predictors. Control variables were significant predictors only in the case of USB since work experience was negatively associated to secure USB use. The results show that there were some similarities in the predictors of ISB but also behavior-related differences were detected. Of the three theories, the constructs from PMT and SOS added significant predictors to the model while DT did not. Sanctions were not significant determinants of ISB in any of the behavioral cases. SOS appeared to explain ISB in two of the cases which indicates that it adds explanatory power to the two more commonly used theories. Problems with multicollinearity weaken the generalizability of these results and need to be considered when interpreting them.

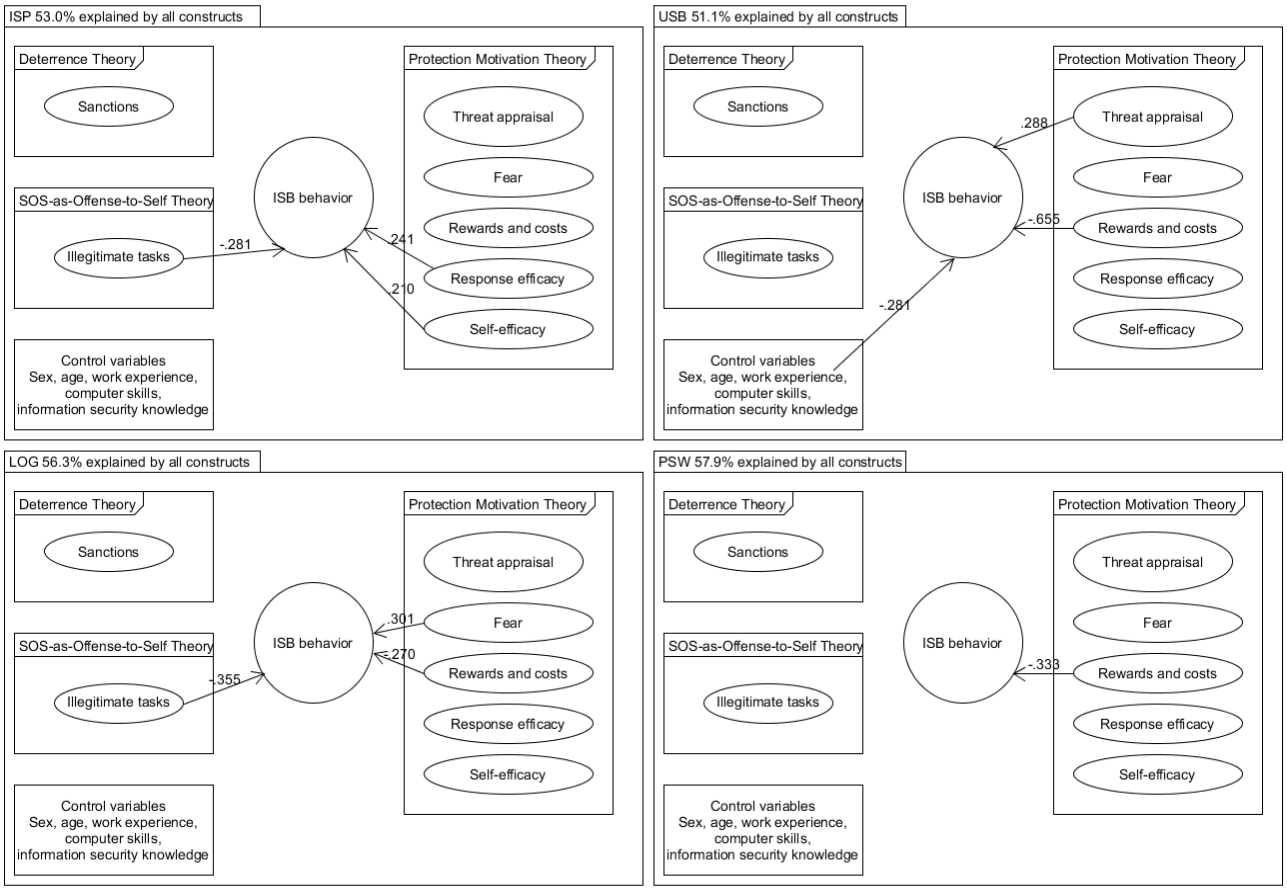

Figure 2 Comparison of the ISBs

Note. Only the significant predictor associations are presented with arrows.

4 DISCUSSION

The aim of the present study was to introduce new explanatory construct, namely illegitimate tasks from Stress-as-Offense-to-Self Theory (SOS), to better understand information security behavior (ISB). With this new construct, more commonly used constructs from Deterrence theory (DT) and Protection Motivation Theory (PMT) were used to explain ISB. In addition, this study used several behaviors separately to evaluate the generalizability of the behavioral determinants. The behaviors studied were general ISP compliance (ISP), not copying sensitive information to the unsecured USB drive (USB), locking or logging out from the computer (LOG), and not writing down passwords (PSW). The background of the participants was rather similar and there were no differences between the behavior-specific questionnaires in sex, age, work experience, or computer skills. This indicates that the found differences between the behaviors were not due to background factors but rather reflect genuine differences between behaviors.

In terms of behavioral determinants, theory-based hypotheses were tested separately for each ISB. In accordance with the assumption of DT (D'Arcy & Herath, 2011; Gibbs, 1975), it was expected that formal (e.g., being subjected to disciplinary actions) and informal (e.g., losing respect and trust of one's supervisor) sanctions increased the probability of secure ISB. Based on the PMT model of the evaluations of threats and possibilities to cope with them (Floyd et al., 2000; Rogers, 1975), it was expected that both higher threat and coping appraisals, as well as fear evoked by the situation, were positively associated to secure ISB. In addition, maladaptive rewards and response costs associated to the behavior were expected to be negatively associated to secure ISB. SOS (Semmer et al., 2007, 2015) was included as a new explanatory theory, since one of its constructs, namely illegitimate tasks, has been noticed to increase the probability of counterproductive work behavior (e.g., deviance from the rules and regulations of the company) (Semmer et al., 2010). Unsecured ISB can be an example of counterproductive work behavior, and it was expected that high amount of illegitimate tasks was negatively associated to secure ISB. These theoretical hypotheses were supported in the cases of certain behaviors and not in the cases of others.

Illegitimate tasks appeared to be a beneficial addition to the explanatory constructs of ISB since they had a strong negative association with two of the ISBs, ISP and LOG. In these cases, they were the strongest determinants of behavior. Secure ISB appears to be less likely when people experience that tasks related to information security should not be expected from them or when they perceive them to be unnecessary altogether. The results were in

accordance with the previous research on associations between counterproductive work behavior and illegitimate tasks (e.g., Semmer et al., 2010, 2015; Stocker et al., 2010). These results were also to some extent comparable to the findings of the role of disengagement strategies (D'Arcy et al., 2014) or neutralization techniques (Siponen & Vance, 2010) in explaining ISP violations, where people can evaluate themselves not to be responsible for violations by shifting blame to someone else. Compared to these strategies and techniques, SOS addresses the process leading from illegitimate tasks to counterproductive behavior. Tasks that are perceived to be illegitimate can be perceived as threats to positive self-image and signs of disrespect towards the person from the organization (Semmer et al., 2007, 2015). When people feel disrespected they are less likely to be good organizational citizens and they can evaluate defying the rules to be legitimate considering the illegitimacy of organization's demands. In the present study, illegitimate tasks were the most prominent determinant of LOG. Especially, in the case of locking or logging out of the computer when leaving the workstation for a short while (e.g. toilet break), it could feel like an illegitimate demand to log out from the computer and then log back in when returning to work a few minutes later.

Illegitimate tasks were highly correlated with rewards and costs from PMT, which were other prominent predictor of ISB in this study. Rewards and costs were significant predictors of behavior in the cases of USB, LOG, and PSW, and their association with ISB was negative, as expected (Floyd et al., 2000). They were the only significant determinant of PSW and the strongest determinant of USB. If the benefits of acting insecurely appear to be higher for the individual or if the secured behavior demands too many resources, unsecured ISB is more probable. High correlation between rewards and costs and illegitimate tasks can be explained by the theoretical expectations of SOS (Semmer et al., 2007, 2015). People's actions are motivated by their evaluations of the task and its effects on themselves. If the task is evaluated to be unfair or redundant, a person can question it and turn to consider the benefits of not acting in a way that is expected. When the task is considered to be illegitimate, the person can justify not doing it by evaluating that it takes too much of one's time and effort to do the task. When the task is illegitimate, the role of maladaptive rewards of not doing it can become central and overcome other factors when determining how to act in a certain situation. These results indicate that it is essential to consider how people experience the pay-off of actions when intending to increase secure behavior.

Although SOS added explanatory power to the understanding of ISB, PMT appeared to be the strongest theory in predicting ISB. Its constructs were significant in all the four ISBs but there were differences in the roles of the constructs in explaining different ISBs. In most of the previous studies, there has been support for the role of both threat and coping appraisal in determining behavior (e.g., Crossler & Bélanger, 2014; Ifinedo, 2012; Workman et al., 2008). The role of rewards and costs have also been noticed in several studies (e.g., Vance et al., 2012). However, there are also many studies in which only a part of theoretically expected associations have been detected or the direction of association have been opposite to the expected (e.g., Herath et al., 2014; Kim et al., 2014; Siponen et al., 2014; Workman, 2009). In the present study, rewards and costs explained the behavior in three of the four cases while the role of the other constructs differed between the cases. It is possible that the discrepancies in the previous research are due to the differential role of determinants regarding different ISBs. In the present study, only the general ISP compliance was predicted by coping appraisal, namely response efficacy and self-efficacy. In turn, threat appraisal and fear were significant predictors of two behaviors, USB and LOG, while PSW was not explained by either.

Based on these results, the role of the appraisals in determining behavior is context-specific, and there are also previous findings that support this notion. Lee and Larsen (2009) have noticed that the role of threat and coping appraisal depended on the expertise level and IT-sensitivity of the industry. The role of the appraisals as predictors of behavior has also varied based on organizational procedural justice (Workman et al., 2009), normative beliefs (Siponen et al., 2006) or habits (Vance et al., 2012). It has also been noticed that the appraisal processes are affected by each other (e.g., Johnston & Warkentin, 2010). In the present study, USB and LOG were predicted by both the evaluations of rewards and costs and fear or threat appraisal. Rewards and costs, on their own or with illegitimate tasks, appeared to have a stronger association with ISB than threat appraisal and fear. It is possible that maladaptive rewards and response costs can overcome threat and fear of the consequences when determining how to act in certain situations. However, the relationships between different determinants should be studied in more detail to determine how they affect each other. For example, Boss et al. (2015) have inspected the effect of fear appeals on other appraisal processes. They noticed that the number of fear appeals changed the relationships between determinants and behavior, indicating that high fear can amplify the significance of threat and coping appraisals as predictors of behavior.

Floyd et al. (2000) dress the importance of environmental cues and previous experiences in determining how people process information and how threat and coping appraisals are formed based on this processing. It is possible that four behaviors investigated in the present study have different associations to people's previous experiences and their evaluations. For example, coping appraisal can be a more prominent determinant of behavior in the case of ISP compliance if the company addresses how well the threats are mitigated by following ISP and offers education that boosts self-efficacy in relation to ISP. In the context of more specific behaviors, like transferring information to USB drives or locking the computer, the threat and fear related to the consequences can be more tangible and this way affects the behavior. Regarding specific behaviors, rewards and costs appeared to outperform other predictors which could be due to being better able to evaluate the rewards and costs in relation to specific behavior than more general rule-following. The role of illegitimate tasks together with PMT constructs was also different in the ISBs. In the case of LOG, the illegitimacy of tasks was evaluated together with rewards and costs and fear while in the case of ISP, response efficacy and self-efficacy affected the behavior together with illegitimacy evaluation.

Based on the results of the present study, DT did not add significant explanatory power when PMT and SOS constructs were included in the models. These findings are in accordance with previous research by Lee et al. (2004), Pahnila et al. (2007a), and Siponen and Vance (2010) where sanctions became insignificant determinants of behavior when other factors, such as neutralization techniques or effectiveness of security systems, were added into the models. However, in many studies there has been an association between sanctions and ISB (e.g., D'Arcy & Devaraj, 2012; Siponen et al., 2010), and especially between informal sanctions and ISB (e.g., Cheng et al., 2013; Guo & Yuan, 2011). In the present study, sanctions were considered as a whole so more elaborate analyses of the importance of formal or informal sanctions were not possible. ISB appears to be better affected by other means than sanctions.

In the present study, the overall explanatory levels for the ISBs all exceeded 50%. Adding illegitimate tasks to the explanatory constructs besides the constructs from DT and PMT yielded higher explanatory levels of actual behavior by other factors than intentions than previous research using DT and PMT jointly (e.g., Herath & Rao, 2009b; Pahnila et al., 2007a,

b, Siponen et al., 2007). This was true especially in the cases of LOG and PSW where the determinants explained nearly 60% of the variance in behavior. In all of the cases, the theoretical constructs outperformed the control variables and only in the case of USB, work experience became significant determinant on its own. More work experience appeared to have a negative association with secure behavior. Overall, the results showed that PMT and SOS are useful theories in explaining different forms of ISB. The behavior-specific results also showed that the significance of the determinants can vary between behaviors. Behavior-specificity of certain determinants could also explain the discrepancies noticed in the previous studies (e.g., Cheng et al., 2013; Herath & Rao, 2009a; Kim et al., 2014; Li et al., 2010; Vance et al., 2012; Workman, 2009). It is also possible that by combining different scenarios to the same models (see e.g., D'Arcy et al., 2014; Siponen & Vance, 2010), the behavior explained does not reflect any actually existing behavior but is an approximation of several behaviors that could be better understood by studying them separately.

4.1 Implications and Limitations of the Study

This study indicates that determinants of ISB can vary depending on the behavior in question and that same determinant could have various roles in explaining different ISBs. Future research should focus on context-specific determinants, as has also been suggested in the guidelines for future research in information security field (Crossler et al., 2013; D'Arcy & Herath, 2011). The results of this study also indicate that illegitimate tasks should be included in the research models explaining ISB since they add explanatory power to previously used determinants and in some cases, they are even the most prominent determinants of ISB. The context-specific determinants of behavior could also be studied in combination with information security management strategies related to employee behavior. For example, the role of fear appears to be different in determining ISBs and it could be that fear-related ISB management strategies could have differing effects depending on if the targeted behavior is password write-down or locking the computer. This kind of research design could also give important ideas for the practice of how to ensure compatibility of behavior management strategies and behaviors that are targeted.

Regarding the practical implications of this research, there is strong indication that different forms of behavior should be managed by different strategies. In previous research, D'Arcy and Hovav (2009) noticed that countermeasures, such as security awareness programs and ISPs, were differently associated with behavioral intentions. In the present study, information security knowledge was not significantly associated to any of the behaviors while the evaluations of task illegitimacy and rewards and costs were important. In the future awareness programs and security education, the importance of employees' actions in taking care of information security could be addressed to help employees to evaluate secure ISB as a relevant part of their job. A new strategy to encourage employees to act securely could be to express appreciation of their role as active agents in improving information security of the company. Possibly rewards of secure behavior could be issued to counter the maladaptive rewards of not following security rules and regulations. Based on the differences in behavioral determinants of different ISBs, determining the compatibility of counter-

measure and behavior in question, better-targeted strategies could be used to improve information security. The knowledge of context-specificity of behavioral determinants could also be used in risk management by focusing on automation of security measures that people are most likely to ignore either based on perceptions of illegitimacy or fear.

The following limitations should be considered when evaluating the results of the present study. The sample sizes for each of the behavior-specific questionnaires were relatively small and there were indications of common method bias and multicollinearity in the sample which restricted the differentiation between determinants of DT, PMT, and SOS, and refrained from using more state-of-the-art analysis tools, like SEM. In the future research, larger samples and measures with better discriminant validity for separate behaviors should be used to investigate if the findings of the present study are replicable with more reliable methods. Furthermore, measures to decrease the effects of common method bias should be applied (Podsakoff et al., 2012). This study measured independent (determinants) and dependent (ISB) variables at the same time. To be able to conclude that independent variables predict the dependent variable, they should be measured at the prior time point to the dependent variable. Longitudinal design should be utilized in the future research. In addition, the sample of the present study was relatively homogenous; the majority of the respondents were young, had relatively little work experience, and were technologically savvy. Because of this, the results of this study are not necessarily generalizable to other populations. The field of the work was also not asked and it is possible that information security issues have a differing role in different fields of work. Although there were problems with the data, the results regarding some form of differences in behavioral determinants of ISB are likely replicable.

4.2 Conclusions

DT, PMT, and SOS, as well as control variables, explained more than half of the variance (51,1-57,9%) in all of the behaviors, namely ISP, USB, LOG, and PSW. Illegitimate tasks had a relatively strong negative association with two of the ISBs indicating that they function as a determinant of ISB and should be considered in the future research of ISB. Illegitimate tasks also added explanatory power to the models containing sanctions from DT and appraisals from PMT. Illegitimate tasks were the strongest determinant of ISP and LOG. Although illegitimate tasks had a significant association with two of the ISBs, PMT contributed the most strongly to explaining different ISBs. Rewards and costs were the most prominent determinants of behavior and they also correlated highly with illegitimate tasks. This association can be theoretically explained and understood by SOS which addresses the effects of task evaluation on one's self-image and relationship with the organization one works at. Of the other constructs of PMT, fear and threat appraisal were significant predictors of LOG and USB, respectively, while response efficacy and self-efficacy predicted ISP. According to the findings of this study, sanctions from DT were not significant predictors of any of the ISBs. The results of the present study indicate that ISB has complex and multiple determinants that differ depending on the behavior in question. Findings related to a certain form of behavior are not necessarily generalizable to explaining other behaviors. This should be taken into account when planning research designs and practical procedures for information security management.

LIST OF REFERENCES

Abraham, S. (2011). Information Security Behavior: Factors and Research Directions. In *AMCIS 2011 Proceedings – All Submissions, 462*.

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

Bernerth, J. B., & Aguinis, H. (2015). A critical review and best-practice recommendations for control variable usage. *Personnel Psychology, 00,* 1-55.

Björk, L., Bejerot, E., Jacobshagen, N., & Härenstam, A. (2013). I shouldn't have to do this: Illegitimate tasks as a stressor in relation to organizational control and resource deficits. *Work & Stress*, *27*(3), 262–277.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations:
An integrated model based on social control and deterrence theory. *computers & securit y*, *39*, 447–459.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, *295*(2), 295–336.

Cisco Systems. (2011). *Cisco connected world technology report.* San Jose, Ca: Cisco Systems.

Crimmins, J. E. (2011). Principles of Utilitarian Penal Law in Beccaria, Bentham and Mill. In P. K. Koritansky (Ed.), *The Philosophy of Punishment and the History of Political Thought* (pp. 136–71). Columbia, Missouri: The University of Missouri Press.

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *ACM SIGMIS Database*, *45*(4), 51–71.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091–1124.

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., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems, 31(2),* 285–318.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, *89*(1), 59–71.

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.

De Cremer, D., & Tyler, T. R. (2005). Am I respected or not?: Inclusion and reputation as issues in group membership. *Social Justice Research*, *18*(2), 121–153.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security*, *20*(8), 715–723.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39–50.

Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, *4*(1), 1-77.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York: Elsevier.

Green, S. B. (1991). How many subjects does it take to do a regression analysis. *Multivariate Behavioral Research, 26*(3), 499–510.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, *49*(6), 320–326.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A Protection Motivation Theory perspective. *Information Systems Management, 33*(1), 2–16.

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

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165.

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

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), 99–110.

Humaidi, N., & Balakrishnan, V. (2015). The moderating effect of working experience on health information system security policies compliance behaviour. *Malaysian Journal of Computer Science*, *28*(2), 70-92.

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

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

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

Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *The Scientific World Journal, 2014.*

Kottwitz, M. U., Meier, L. L., Jacobshagen, N., Kälin, W., Elfering, A., Hennig, J., & Semmer, N. K. (2013). Illegitimate tasks associated with higher cortisol levels among male employees when subjective health is relatively low: an intra-individual analysis. *Scand J Work Environ Health*, *39*(3), 310–318.

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

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, *50*(2), 361–369.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187.

Lee, S. M., Lee, S. G., & 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., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*(4), 635–645.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293–334.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Madsen, I. E., Tripathi, M., Borritz, M., & Rugulies, R. (2014). Unnecessary work tasks and mental health: a prospective analysis of Danish human service workers. *Scandinavian Journal of Work and Environmental Health*, *40*(6), 631–638.

Metsämuuronen, Jari. (2005). *Tutkimuksen tekemisen perusteet ihmistieteissä* (3rd ed.). Jyväskylä: Gummerus.

Muthén, L.K. & Muthén, B.O. (1998-2012). *Mplus user's guide* (7th ed.). Los Angeles, CA: Muthén & Muthén.

Nunnally, J. C., & Bernstein, I. H. (1994). The assessment of reliability. *Psychometric Theory*, *3*(1), 248-292.

Pahnila, S., Siponen, M., & Mahmood, A. (2007a). Employees' behavior towards IS security policy compliance. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 156b–156b). IEEE.

Pahnila, S., Siponen, M., & Mahmood, A. (2007b). Which factors explain employees' adherence to information security policies? An empirical study. *PACIS 2007 Proceedings*, 73.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, 549–583.

Peeters, M. C., Buunk, B. P., & Schaufeli, W. B. (1995). Social interactions and feelings of inferiority. *Journal of Applied Social Psychology*, *25*(12), 1073–1089.

Pereira, D., Semmer, N. K., & Elfering, A. (2014). Illegitimate tasks and sleep quality: An ambulatory study. *Stress and Health*, *30*(3), 209–221.

Piquero, A., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly*, *13*(3), 481–510.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology, 63*, 539–569.

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2006). The empirical status of deterrence theory: A meta-analysis. In F.T. Cullen, J.P. Wright, & K.R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 37–76). New Brunswick, NJ: Transaction.

Puhakainen, P. (2006). Design theory for information security awareness. Oulu, Finland: University of Oulu.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114.

Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online*, *8*(2), 23–74.

Semmer, N. K., Jacobshagen, N., Meier, L. L., & Elfering, A. (2007). Occupational stress research: The "stress-as-offense-to-self" perspective. *Occupational Health Psychology: European Perspectives on Research, Education and Practice*, *2*, 43–60.

Semmer, N. K., Jacobshagen, N., Meier, L. L., Elfering, A., Beehr, T. A., Kälin, W., & Tschan, F. (2015). Illegitimate tasks as a source of work stress. *Work & Stress*, *29*(1), 32–56.

Semmer, N. K., Tschan, F., Meier, L. L., Facchin, S., & Jacobshagen, N. (2010). Illegitimate tasks and counterproductive work behavior. *Applied Psychology*, *59*(1), 70–96.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224.

Siponen, M., Pahnila, S., & Mahmood, A. (2006, November). Factors influencing protection motivation and IS security policy compliance. In*Innovations in Information Technology, 2006* (pp. 1–5). IEEE.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In *New approaches for security, privacy and trust in complex environments* (pp. 133–144). US: Springer.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: an empirical investigation. *Computer*, *43*(2), 64–71.

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

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. In ICIS 2008 Proceedings, 26.

Spector, P. E., & Fox, S. (2002). An emotion-centered model of voluntary work behavior: Some parallels between counterproductive work behavior and organizational citizenship behavior. *Human Resource management review*,*12*(2), 269–292.

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

Stocker, D., Jacobshagen, N., Semmer, N. K., & Annen, H. (2010). Appreciation at work in the Swiss armed forces. *Swiss Journal of Psychology, 69*(2), 117–124.

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

Thomson, K. L., & Von Solms, R. (2005). Information security obedience: a definition. *Computers & Security*, *24*(1), 69–75.

Tracy, J. L., & Robins, R. W. (2004). " Putting the Self Into Self-Conscious Emotions: A Theoretical Model". *Psychological Inquiry*, *15*(2), 103–125.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190–198.

van Schie, S., Güntert, S. T., & Wehner, T. (2014). How dare to demand this from volunteers! The impact of illegitimate tasks. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations*, *25*(4), 851–868.

von Solms, S. B. (2005). Information Security Governance–Compliance management vs operational management. *Computers & Security*, *24*(6), 443–447.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376.

Whitman, M., & Mattord, H. (2013). *Management of Information Security*. Cengage Learning.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health, Education & Behavior*, *27*(5), 591–615.

Workman, M. (2009). How perceptions of justice affect security attitudes: suggestions for practitioners and researchers. *Information Management & Computer Security*, *17*(4), 341–353.

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