Why Deterrence is not Enough: The Role of Endogenous Motivations on Employees’ Information Security Behavior

Abstract

Information systems security (ISS) is an increasingly critical issue for companies worldwide. In 2013 cybercrime has caused losses worth US $113 billion affecting 378m victims (Norton Symantec Cybercrime Report 2013). Besides criminal attacks and system malfunctions, human error is the major reason for information security incidents. Hence, refining our understanding how employees’ behavior regarding information security can be explained and influenced is a top priority in academia and business practice (D’Arcy et al. 2009; Siponen and Vance 2010). In this respect, numerous studies have examined the role of deterrence mechanisms such as monitoring or sanctioning on individual security compliance. A perspective largely neglected by prior research is the role of endogenous motivations (Siponen and Oinas-Kukkonen 2007), although studies in adjacent fields have shown the effectiveness of motivational intervention strategies (Wunderlich et al. 2013). Our study seeks to close this gap by examining how endogenous motivations influence individual ISS-related behavior. Our proposed model integrates the theory of planned behavior (TPB) and the organismic integration theory (OIT) – a sub-theory of the self-determination theory (SDT). We empirically test the model using a sample of 444 employees from different organizations. The results show that when employees’ personal values and principles are congruent with their employer’s ISS-related prescriptions and goals their intention to comply with security policies significantly increases. On the contrary, we find no impact on compliance intention when employees perceive their actions as a result of external pressures and coercion. The study’s findings advance our understanding of the motivational processes underlying security compliant behavior and provide numerous implications for researchers and practitioners.

Keywords: Information systems security, information security behavior, organismic integration theory, self-determination theory, theory of planned behavior, endogenous motivation
Introduction

According to Norton Symantec Cybercrime Report (2013) 378 million people have been marred by cybercrime in the past year, causing losses of US $113 billion. The main reason for security breaches are malicious attacks, system glitches, and mistakes by employees. For hackers, employees represent popular targets to intrude a company’s network as it is estimated that around 20 percent of employees enter their usernames and passwords in response to faked “phishing” e-mails, which pretend to come from legitimate sources (The Economist 2014). Recent studies estimate that more than 50 percent of all ISS incidents in organizations are the direct or indirect consequence of employees’ misbehavior (Ernst and Young 2005, Siponen and Vance 2010). On the average a company loses US $277 for each user’s account put at risk. With the number of threats and their severity of consequences rising, avoiding information systems security (ISS) incidents is becoming a major challenge for organizations (Gordon et al. 2011). As a result, large companies reportedly spent more than $32.8 billion on ISS in 2012 according to International Data Corporation, a research firm (Chen et al. 2012). Small- and medium-size organizations are even expected to spend more on ISS than on other IS/IT over the next three years (Perlroth and Rusli 2012). The investments often focus on technological remedies such as encryption, anti-spyware, virus detection, or firewalls (Spears and Barki 2010). However, without training employees on how to recognize malicious attacks and avoid unintentional errors, organizations cannot succeed in information security (Siponen 2000, Son and Rhee 2007, Boss et al. 2009, Bulgurcu et al. 2010). Although most companies regularly offer security education, training and awareness (SETA) programs to employees, the success of these programs is limited due to a lack of engagement and participation. Practitioners and researchers alike are thus interested in how to improve employee engagement and motivation to comply with organizational ISS guidelines (Siponen and Oinas-Kukkonen 2007, Bulgurcu et al 2010, Johnston and Warkentin 2010).

Numerous previous studies on IS security have focused on deterrence mechanisms to explain why employees do or do not adhere to information security policies (ISPs) (e.g., D’Arcy and Hovav 2007, D’Arcy et al., 2009, Herath and Rao 2009a and 2009b, Workman et al. 2009, Siponen et al. 2006, 2010). Those studies implicitly suggest that extrinsic motivations, e.g., avoidance of sanctions, are the major motivation for employees to comply with organizational security guidelines. Another stream of motivational ISS studies, which is largely based on protection motivation theory (PMT), investigated intrinsic factors such as employees’ perceived effectiveness of information security behavior, perceived intrinsic costs or benefits of ISP compliance (Bulgurcu et al. 2010), or the perceived mental pleasure of committing the intended act (Hu et al. 2011). However, traditional motivational studies predominantly followed mechanistic motivation theories, which contend that behaviors are either being triggered extrinsically by rewards or intrinsically when the activity itself is the reward (exogenous motivation). To the best of our knowledge these studies have not differentiated between different forms of extrinsic motivation ranging from external to internal perceived locus of causality. Self-determination theory (SDT) and its sub-theory the organismic integration theory (OIT) in contrast consider these subtypes of extrinsic motivation, which fall along the continuum of internalization (Deci and Ryan 2002; Ryan and Deci 2000). The more an individual has internalized an external regulation (e.g. ISP), the more autonomous she/he will perceive the compliance with this regulation. According to SDT/OIT, an individual’s perception of autonomy, competence, and relatedness will increase an individual’s motivation to perform a particular behavior with enhanced performance, persistence, and creativity. OIT particularly focuses on an individual’s psychological need for autonomy when performing a behavior and considers human actions not as a consequence of expected incentives (exogenous motivation), but rather by the subjective psychological meaning of these stimuli (endogenous motivation).

Our study employs this organismic perspective to augment our understanding regarding the impact of employees’ endogenous motivation on their intention to comply with ISPs. Thereby we address a gap in the literature regarding the role of internalization, i.e. the integration of organizational security standards and values into one’s own sense of self (Layton 2005, Siponen and Oinas-Kukkonen 2007). We expect that the extent to which employees comprehend and internalize security policies and values influences their motivation to comply with ISPs. We develop and empirically validate a research model that integrates SDT/OIT with the theory of planned behavior (TPB) (Ajzen 1991). According to Vallerand’s (1997) hierarchical model of motivation, the two theories provide complementary explanations: While the TPB is appropriate to explain specific target behaviors, SDT/OIT constructs represent individuals’ general motivations in a specific context. Although the TPB and SDT/OIT are each well studied on its
own, this study is the first to integrate them in the context of ISS research. Combining both theories provides valuable insights on how perceived self-determination and internalization of security policies affect ISS-related behaviors.

The remainder of the study is organized as follows. Next, we give a background overview of prior research on ISS behavior. We then develop the hypotheses and present the proposed research model. After describing the research methodology, we will present the results of the statistical analyses. Finally, we discuss the results, provide theoretical and practical implications, refer to the study’s limitations and give recommendations for future research.

**Background**

To explain employees’ motivation to comply with ISPs, the general deterrence theory (GDT) has been the dominating theoretical perspective (Siponen and Vance 2010). Originating in the field of criminal science, GDT contends that ISP compliance is largely driven by threats of sanctions for ISP violations and the IS end-users’ perceived certainty and severity of those sanctions. Building upon the GDT, D’Arcy and Hovav (2007) and D’Arcy et al., (2009) show that employees’ awareness of security countermeasures such as ISPs, SETA programs, and monitoring activities positively influence the perceived severity and certainty of organizational sanctions associated with IS misuse and therefore indirectly tend to reduce IS misuse intention. D’Arcy et al. (2009, p. 80) contend that “from a deterrence perspective, security policies rely on the same underlying mechanism as societal laws: providing knowledge of what constitutes unacceptable conduct increases the perceived threat of punishment for illicit behavior”. However, the effectiveness of deterrence mechanisms has often been questioned since a variety of studies report inconclusive results (D’Arcy and Herath 2011). Hu et al. (2011) and Pahnila et al. (2007a) did not find evidence for threats of sanctions significantly affecting employees’ ISP compliance. Similarly, Guo et al. (2011) found no evidence that employees’ perceived certainty of sanctions prevents ISP violation. Also implementing deterrence security mechanisms such as computer monitoring and sanctioning for ISP violations did not reduce the quantity and severity of ISS breaches (Wiant 2005). With regard to other extrinsic motivations such as avoiding shame, informal penalties, or rewards the literature reports moderate or non-significant effects on individual ISP compliance (Pahnila et al. 2007b, Siponen and Vance 2010, Liang et al. 2013). Some scholars have even suggested that extrinsic motivations may negatively affect security behavior (Benabou and Tirole 2003). In his conceptual paper Siponen (2000) suggests considering personality traits such as morals, ethics, emotions, well-being and a feeling of security as important factors influencing individual motivations to act in accordance with organizational security guidelines. In a similar direction further studies indicate that intrinsic and affirmative mechanisms ensuring commitment and participation such as the perceived mental pleasure of committing the intended act (Hu et al. 2011), employees’ perceived effectiveness of security behavior (Herath and Rao 2009a), organizational commitment (Herath and Rao 2009b), perceived legitimacy (Son and Rhee 2011), perceived intrinsic benefits (Bulgurcu et al. 2010), or the perceived fairness of the requirements of the ISPs (Bulgurcu et al 2009) positively affect employees’ ISP compliant behavior.

These studies provide important insights on the role of extrinsic and intrinsic motivations, however to our best knowledge no study exists that delves more deeply into the role of endogenous motivations on ISP compliance behavior. Recent research on the SDT and OIT (see Ryan and Deci 2000, Deci and Ryan 1985 and 2002) in IS research (Malhotra et al. 2008, Wunderlich et al. 2013) and other domains such as marketing (Cadwallader et al. 2010) and health behavior (Hagger and Chatzisarantis 2009) suggest that an individual’s perceived autonomy in initiating a behavior directly impacts the likelihood that this behavior is actually performed. In particular these studies found that if externally prescribed rules are congruent with individual values (internalization), following those rules is perceived as autonomously driven, which in turn leads to a higher likelihood of individuals to comply. External stimuli (e.g. ISPs) than have similar effects as intrinsic motivations. This is the difference between OIT and mechanistic motivational studies, which solely differentiate between extrinsic and intrinsic motivation. Thereby OIT particularly focuses on the antecedents and impacts of different forms of extrinsic motivation including external regulation as measured by the construct external PLOC (low internalization) and identification and integration as measured by internal PLOC (high internalization). External and internal PLOC are the end points of the internalization continuum. The more an extrinsic motivation is internalized, the more autonomous an individual will perceive her/his behavior. Therefore, OIT is particularly suited to...
understand how extrinsic motivations regarding IS security influence the internalization of goals and norms included in organizational ISPs which can lead to resistance, partial compliance, or full internalization of IS security goals.

Theoretical Framework and Hypotheses

Theory of Planned Behavior

The TPB (Ajzen 1991) has been proven to be a compelling social cognitive framework to explain situation-specific influences on intentional behaviors across a variety of disciplines. TPB claims that human behavior is essentially rational and largely relies on an individual’s intention. According to the TPB, the prediction of intention relies on three belief-based variables: Attitude towards the behavior, normative beliefs, and perceived behavioral control (Ajzen 1991). Consistent with the literature we used self-efficacy instead of perceived behavioral control “...because the latter essentially measures the same latent construct as self-efficacy (Fishbein 2007) and it originates from self-efficacy theory (Bandura 1977)” (Bulgurcu et al. 2010, p. 528). In the context of our study, attitude towards ISP compliance refers to the degree to which an individual thinks it is personally favorable or unfavorable to comply with the ISP (Fishbein and Ajzen 1975, Bulgurcu et al 2010). Self-efficacy can be defined as “an employee’s judgment of personal skills, knowledge or competency about fulfilling the requirements of the ISP” (Bandura 1977, Bulgurcu et al. 2010, p. 529). Normative beliefs are defined as “an employee’s perceived social pressure about compliance with the requirements of the ISP caused by behavioral expectations of such important referents as executives, colleagues, and managers” (Ajzen 1991, Bulgurcu et al. 2010, p. 529). Based on broad empirical evidence that the TPB constructs are strong predictors of behavioral intention (Pahnila 2007a, Herath and Rao 2009a and 2009b, Bulgurcu et al. 2010), we state the following hypotheses:

H1: Attitude towards ISP compliance positively influences an individual’s intention to comply with the ISP.

H2: Self-efficacy to comply with ISP positively influences an individual’s intention to comply with the ISP.

H3: Normative beliefs about ISP compliance positively influence an individual’s intention to comply with the ISP.

Self-Determination and Organismic Integration Theory

Hitherto, the ISS literature predominantly understood motivation from a mechanistic perspective differentiating solely between extrinsic or intrinsic motivations. This perspective considers motivation to differ only in terms of amount (e.g. Bandura 1996), meaning that more motivated individuals “will aspire to greater achievement and be more successful in their efforts than people with less motivation” (Cadwallader et al. 2010, p. 221). In contrast, OIT which is a sub-theory of SDT contends that the quality of motivation—exogenous vs. endogenous—is more important than the mere amount of motivation (see Deci and Ryan 2002; Ryan and Deci 2000b). This means that from an organismic perspective the same external stimuli (e.g. prescribed rules within ISPs) may motivate different behavioral responses depending on one’s endogenous psychological feelings of autonomy or pressure with regard to the stimuli. OIT conceives behavior as either autonomously motivated such that people perceive the behavior as initiated by choice of the self or controlled when a behavior is perceived as externally enforced (Deci et al. 1991, 2000).

To analyze an individual’s perceived degree of autonomy, the OIT distinguishes between the internal and external perceived locus of causality (PLOC) (Ryan and Connell 1989). The PLOC taxonomy is based on the theory of internalization which describes “… a continuum in which a social value or regulation is adopted as one’s own or identified with” (Ryan and Connell 1989). Internalization of external regulations results in that these regulations are fully endorsed by the self (Deci et al. 1991). Hence, the more an external regulation is appropriated and internalized, the higher is the perceived level of autonomy in complying with this regulation (Ryan and Connell 1989). This contrasts OIT from SDT, which solely considers different degrees of perceived autonomy but does not build on the process of internalizing external regulations. Obeying to rules under the influence of internal PLOC is thus caused by endogenous motivation that result from an individual’s appraisal of the behavior in question as being personally
meaningful and therefore rely to intrinsic motivation although the stimuli (e.g. ISP) seems to be of extrinsic nature (Malhotra et al. 2008). In contrast, external PLOC refers to extrinsic motivation in its purest form in that individuals that are motivated through external PLOC perceive their behavior as being controlled by external forces (Ryan and Connell, 1989).

<table>
<thead>
<tr>
<th>Figure 1. Endogenous motivation (adopted from Ryan and Connell 1989, Ryan and Deci 2000)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Non-Self Determined</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>Extrinsic Motivation</td>
</tr>
<tr>
<td>External PLOC</td>
</tr>
</tbody>
</table>

**Integrating the Theory of Planned Behavior and Organismic Integration Theory**

Both the TPB and SDT/OIT aim to explain human behavior. However, they differ in their level of generality (Vallerand 1997). While, the TPB refers to a particular behavior, SDT/OIT relates an individual’s general motivations in a given context (Deci and Ryan, 1985, Ryan and Connell, 1989). Hence, PLOC influences behavior not only through “the here and now of motivation” (Vallerand 1997, p. 293), but beyond that is suggested to affect various behaviors in particular contexts through more generalized motivations (Cadwallader et al. 2010, Wunderlich et al. 2013). In this regard, a connection can be drawn to Vallerand’s (1997, 2000) hierarchical model of motivation, which suggests that due to the different degree of generality of contextual and situational motivations, the first affects the latter in a top-down fashion (Hagger et al. 2006, Wunderlich et al. 2013).

Internal PLOC results from a high level of internalization of external regulations (Ryan and Connell 1989). If employees internalize the rules prescribed in the ISP, they adopt the regulation as their own and identify themselves with it because it is perceived as personally important and congruent with their own values (Ryan and Connell 1989). Thus, if an employee internalizes external regulations such as guidelines specified in ISPs, the likelihood of ISP-compliant behavior increases since it is perceived as autonomous and personally relevant (Deci and Ryan 1985, Malhotra et al. 2008). Literature suggests that individuals perceiving themselves as the origin of their behavior will make great efforts and sacrifices to perform the behavior (Ryan and Deci 2000, Deci and Ryan 2002, Turban et al. 2007). Hence, we suggest:

H4: Internal PLOC positively influences an individual’s intention to comply with the ISP.

According to the TPB, the attitude towards a behavior is defined as an individual’s evaluation of performing a specific future behavior as desirable (positive) or undesirable (negative) (Fishbein and Ajzen 1975, Malhotra et al. 2008). Prior research in other domains found that a high level of internal PLOC positively influences the attitude towards the respective behavior (Hagger et al. 2006, Wunderlich et al. 2013). We expect that employees having internalized the security guidelines perceive compliance to be necessary and beneficial for them and their organization. Thus, we propose:

H5: Internal PLOC positively influences an individual’s attitude towards ISP compliance.

Self-efficacy describes an individual’s evaluation of one’s own abilities and resources with respect to a specific behavior (Bandura 1977). Individuals who have internalized external regulations (e.g. prescribed rules) usually aim at finding out how to fulfill those regulations (Ryan and Connell 1989). Turban et al. (2007) investigated the effects of PLOC in the context of work task performance and found that individuals with a high level of internal PLOC use their cognitive capabilities more intensively and that they are motivated to acquire the required know-how to perform the expected task. This should lead to higher levels of self-efficacy. Accordingly, for our study we expect that employees with a high level of value
congruence of the rules prescribed in the ISP with their own values strive more thoroughly to acquire the competences needed to avoid unintentional misbehavior. Thus, we contend:

H6: Internal PLOC positively influences an individual’s self-efficacy to comply with the ISP.

External PLOC refers to the least autonomous form of extrinsic motivation. Accordingly, behavior motivated through external PLOC is a result of an individual’s attainment (e.g., rewards) or avoidance of negative consequences (e.g., sanctions) administered by others (Deci and Ryan 1985). This kind of motivation does not rely on self-endorsement, but on motives attributed to external authority or compliance (Ryan and Connell, 1989). GDT claims that the perceived certainty and severity of sanctions for policy violations increases employees’ compliance behavior. These deterrence mechanisms pertain to the external PLOC. Although, deterrence mechanisms limit one’s autonomy, they should still have a positive impact on ISP compliance as extrinsic motives, e.g., avoiding sanctions, may still be important for employees. However, under the influence of external PLOC external regulations are not internalized so that we assume that the effect of external PLOC on intention to comply will be weaker than that of internal PLOC (Ryan and Connell 1989, Dholakia 2006, Malhotra et al. 2008). Hence, we state:

H7: External PLOC positively influences an individual’s intention to comply with the ISP, however to a weaker extent than internal PLOC.

Even though individuals perceive their behavior as externally regulated, they could still value the outcome of the behavior such as avoiding penalties for ISS-related misconduct or being esteemed by colleagues and superiors (Deci and Ryan 1985). Accordingly, even though employees may perceive their security-related behavior as non-autonomous and externally regulated, they may still appreciate the personal or organizational benefits and usefulness of ISP compliance. Therefore, employees might consider complying to ISPs as forced, however still doing it as they profit from it. However, we expect the effects to be weaker than for internal PLOC since attitude formation is influenced by extrinsic motivators (Ryan and Connell 1989, Malhotra et al. 2008). Thus, we expect:

H8: External PLOC positively influences an individual’s attitude towards ISP compliance, however to a weaker extent than internal PLOC.

**Research Methodology**

**Sample and Data-collection Procedure**

To test our model we conducted an online survey. Subjects were recruited by e-mail and posting links using multiple distribution channels such as on- and offline business networks, business portals, and university alumni associations. Web-logs indicated that from 980 initial visitors 578 completed the survey. From this sample we excluded respondents who were self-employed or unemployed (n = 56) and whose employer did not define explicit ISPs (n = 54). We then eliminated answers from respondents with implausible short handling time to avoid untrustworthy click-through answers (n = 24). A detailed examination of the plausibility of response schemes resulted in an elimination of further 14 cases. The final sample size consisted of 444 respondents. Sample demographics are summarized in Table 1.
Table 1. Demographics of Participants

<table>
<thead>
<tr>
<th>Total Sample</th>
<th>n = 444</th>
<th>Percentage</th>
<th>(4) Work Experience</th>
<th>n = 444</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Gender</td>
<td></td>
<td></td>
<td>(4) Work Experience</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>307</td>
<td>69.1%</td>
<td>Min</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>137</td>
<td>30.9%</td>
<td>Max</td>
<td>46</td>
<td></td>
</tr>
<tr>
<td>(2) Age</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Min</td>
<td>20</td>
<td></td>
<td>&lt; 2 years</td>
<td>65</td>
<td>14.6%</td>
</tr>
<tr>
<td>Max</td>
<td>67</td>
<td></td>
<td>3-5 years</td>
<td>124</td>
<td>27.9%</td>
</tr>
<tr>
<td>Mean</td>
<td>35.34</td>
<td>9.0%</td>
<td>6-10 years</td>
<td>86</td>
<td>19.3%</td>
</tr>
<tr>
<td>20-25</td>
<td>40</td>
<td></td>
<td>11-15 years</td>
<td>64</td>
<td>14.4%</td>
</tr>
<tr>
<td>26-35</td>
<td>232</td>
<td>52.3%</td>
<td>16-20 years</td>
<td>34</td>
<td>7.6%</td>
</tr>
<tr>
<td>36-45</td>
<td>106</td>
<td>23.8%</td>
<td>&gt; 20 years</td>
<td>71</td>
<td>15.9%</td>
</tr>
<tr>
<td>46-55</td>
<td>54</td>
<td>12.1%</td>
<td>&lt; 100 employees</td>
<td>81</td>
<td>18.2%</td>
</tr>
<tr>
<td>56-65</td>
<td>10</td>
<td>2.2%</td>
<td>100-499</td>
<td>103</td>
<td>23.1%</td>
</tr>
<tr>
<td>66 and over</td>
<td>2</td>
<td>.4%</td>
<td>500-999</td>
<td>29</td>
<td>6.5%</td>
</tr>
<tr>
<td>(3) Industry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consulting</td>
<td>36</td>
<td>8.1%</td>
<td>1.000-2.499</td>
<td>40</td>
<td>9.0%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>26</td>
<td>5.8%</td>
<td>2.500-9.999</td>
<td>66</td>
<td>14.8%</td>
</tr>
<tr>
<td>IT and Telecom.</td>
<td>117</td>
<td>26.3%</td>
<td>more than 9.999</td>
<td>125</td>
<td>28.1%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>42</td>
<td>9.4%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>223</td>
<td>50.2%</td>
<td>(6) IT Job Function</td>
<td>73</td>
<td>16.4%</td>
</tr>
</tbody>
</table>

Measurement of Constructs

We applied standard psychometric scale development procedures. All latent variables were measured reflectively with multiple items on seven-point Likert-scales with different poles as described in Table 2. The dependent variable intention to comply as well as the constructs of the TPB were adopted from Bulgurcu et al. (2010) who adapted Ajzen’s constructs for the context of ISP compliance. For the two scales capturing the internal and external PLOC, we drew on the measures of Ryan and Connell (1989), which have been adapted to the IS-context by Malhotra et al. (2008) and Wunderlich et al. (2013) and adapted them to fit the context of our study. We conducted qualitative and quantitative pilot studies to validate the items for the scales including sorting procedures with subsequent interviews of four practitioners and six scholars (Moore and Benbasat 1991). Based on the feedback of two pre-tests (n = 25) the wording and order of some items were revised. The instrument along with its psychometric properties is depicted in Table 2.
**Table 2. Measurement items and item loadings**

<table>
<thead>
<tr>
<th>Construct (Source)</th>
<th>Items</th>
<th>Scale</th>
<th>Factor Loading</th>
</tr>
</thead>
</table>
| **Internal Perceived Locus of Causality** (Ryan and Connell 1989) | I comply with the requirements of the ISP...  
(1) ...because I want to ensure the ISS of my employer.  
(2) ...because I think ISS is important.  
(3) ...because I want to find out how to ensure ISS.  
(4) ...because I think it is important to comply with the ISP.  
(5) ...because I would not want to violate the ISP. | a | .858** |
| | | a | .807** |
| | | a | .622**† |
| | | a | .828** |
| | | a | .766** |
| **External Perceived Locus of Causality** (Ryan and Connell 1989) | I comply with the requirements of the ISP...  
(1) ...because I will get in trouble if I do not.  
(2) ...because that is what I am supposed to do.  
(3) ...so that my boss does not penalize me.  
(4) ...because that is the rule.  
(5) ...so others will not get mad on me. | a | .801** |
| | | a | .805** |
| | | a | .705** |
| | | a | .841** |
| | | a | .538**† |
| **Attitude towards ISP compliance** (Ajzen 1991; Bulgurcu et al. 2010) | To me, complying with the requirements of the ISP is _________.  
(1) unnecessary...necessary  
(2) unbeneficial...beneficial  
(3) unimportant...important  
(4) useless...useful | b | .846** |
| | | b | .696** |
| | | b | .860** |
| | | b | .840** |
| **Self-Efficacy to comply** (Ajzen 1991; Bulgurcu et al. 2010) | I have the necessary ______ to fulfill the requirements of the ISP.  
(1) skills  
(2) knowledge  
(3) competencies | c | .946** |
| | | c | .907** |
| | | c | .934** |
| **Normative Beliefs** (Ajzen 1991; Bulgurcu et al. 2010) | ______ think that I should comply with the requirements of the ISP.  
(1) My colleagues  
(2) My executives  
(3) My managers | a | .849** |
| | | a | .931** |
| | | a | .800** |
| **Intention to comply** (Ajzen 1991; Bulgurcu et al. 2010) | (1) I intend to comply with the requirements of the ISP of my organization in the future.  
(2) I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.  
(3) I intend to carry out my responsibilities prescribed in my organization’s ISP when I use information and technology in the future. | a | .969** |
| | | a | .945** |
| | | a | .960** |

**p < .001; † removed items; Scale a: Seven-point Likert scale: (1) = strongly disagree ... (7) = strongly agree; Scale b: Seven-point Likert scale: (1) = extremely; (2) = quite; (3) = slightly; (4) = neither; (5) = slightly; (6) = quite; (7) = extremely; scale c: Seven-point Likert scale: (1) = almost never; (2) = very rarely; (3) = rarely; (4) = occasionally; (5) = frequently; (6) = very frequently; (7) = almost always.**
Analyses and Results

We validated our research model using structural equation modeling. In order to evaluate the psychometric measurement scales and to test the hypotheses we applied the component-based partial least square (PLS) approach using SmartPLS version 2.0.M3 (Ringle et al. 2005). The PLS method was chosen because it is known for its ability to test complex latent variable-based structural equation models with a minimum of methodological requirements and providing robust results (Johnson et al. 2006, Mayfield and Mayfield 2012). Following the two-step approach suggested by Anderson and Gerbing (1988), we first assessed the measurement model and subsequently tested the hypotheses with the structural model.

Assessment of Measurement Model

As shown in Table 2 all items loaded significantly on their underlying latent variable with values well above the recommended threshold of .707 (Chin 1998, Johnson et al. 2006) except of two items (internal PLOC_03 (.62) and external PLOC_03 (.54)), which were therefore eliminated from the measurement model. In order to verify construct reliability (CR), we assessed composite reliability scores, which all exceeded the recommended threshold of .70 (Gefen and Straub 2005) (see Table 3). Further, Cronbach’s alpha values of all constructs were above the threshold of .70. Furthermore, we conducted a confirmatory factor analysis to check cross-loadings. All indicator items loaded significantly more on their corresponding construct than on any other construct. The results imply that the criteria for indicator and construct reliability are met. In a next step, we assessed the convergent validity by examining the constructs’ average variance extracted (AVE). As presented in Table 3, results revealed that the AVE of each construct was well above the common threshold of .50 (Bhattacherjee and Premkumar 2004). We tested discriminant validity applying the criterion of Fornell and Larcker (1981). All correlations between any two constructs were lower than the square root of the corresponding AVE indicating that discriminant validity could also be established.

Table 3. Composite Reliability, AVE, and Latent Variable Correlations

<table>
<thead>
<tr>
<th>Variable</th>
<th>Range</th>
<th>Mean</th>
<th>SD</th>
<th>CR</th>
<th>CA</th>
<th>AVE</th>
<th>IPLOC</th>
<th>EPLOC</th>
<th>ATT</th>
<th>SEE</th>
<th>NOB</th>
<th>INT</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPLOC</td>
<td>1-7</td>
<td>5.828</td>
<td>1.033</td>
<td>.894</td>
<td>.842</td>
<td>.679</td>
<td>.824</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EPLOC</td>
<td>1-7</td>
<td>4.506</td>
<td>1.411</td>
<td>.867</td>
<td>.807</td>
<td>.622</td>
<td>.325</td>
<td>.788</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATT</td>
<td>1-7</td>
<td>5.724</td>
<td>1.092</td>
<td>.886</td>
<td>.830</td>
<td>.661</td>
<td>.622</td>
<td>.262</td>
<td>.813</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEE</td>
<td>1-7</td>
<td>5.949</td>
<td>1.089</td>
<td>.950</td>
<td>.921</td>
<td>.864</td>
<td>.379</td>
<td>.052</td>
<td>.289</td>
<td>.929</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOB</td>
<td>1-7</td>
<td>5.592</td>
<td>1.309</td>
<td>.896</td>
<td>.825</td>
<td>.742</td>
<td>.446</td>
<td>.332</td>
<td>.549</td>
<td>.310</td>
<td>.862</td>
<td></td>
</tr>
<tr>
<td>INT</td>
<td>1-7</td>
<td>6.044</td>
<td>1.038</td>
<td>.971</td>
<td>.955</td>
<td>.918</td>
<td>.638</td>
<td>.249</td>
<td>.611</td>
<td>.345</td>
<td>.530</td>
<td>.958</td>
</tr>
</tbody>
</table>

SD = Standard Deviation; CR = Composite Reliability; CA = Cronbach Alpha; AVE = Average Variance Extracted; IPLOC = internal perceived locus of causality; EPLOC = external perceived locus of causality; ATT = Attitude; SEE = Self-efficacy; NOB = normative beliefs; INT = intention to comply. Diagonal elements represent the square-root of AVE.

Testing the Structural Model

To validate the research model we used structural equation modeling. The significance of the parameter estimates was calculated using bootstrapping with 3,000 samples (Chin 1998). The model could explain a substantial portion of the variance in the dependent variable intention to comply (R² = .520). The results show (see Figure 3) that the TPB’s constructs, attitude ($\beta = .242$, $p<.001$), self-efficacy ($\beta = .084$, $p<.05$), and normative beliefs ($\beta = .216$, $p<.001$) have a positive effect on intention to comply. Hence, the hypotheses H1, H2, and H3 were supported by our data. Likewise, we found H4, H5 and H6 are statistically significant. Internal PLOC has a positive effect on intention ($\beta = .355$, $p<.001$), attitude ($\beta = .600$, $p<.001$), and self-efficacy ($\beta = .379$, $p<.001$). Regarding external PLOC we found no evidence for a positive impact on intention (H7, $\beta = -.007$, $p>.05$), but a significant influence on attitude towards ISP compliance ($\beta = .067$, $p<.05$) supporting hypothesis H8. To test whether or not the effects of EPLOC on intention and on attitude are significantly weaker than the effects of IPLOC on intentions and attitude, we
ran paired-sample t-tests on the bootstrapped path coefficients as suggested by Sarstedt and Wilczynski (2009). The results indicate that both the differences in the path coefficients from EPLOC and IPLOC on intention as well as the differences in the path coefficients from EPLOC and IPLOC on attitude are significant at a level of p<.001. None of the control variables depicted in figure 2 were found to be significant. Since independent and dependent variables were measured within the same instrument at the same time, we also tested for common method bias applying both the Harman’s single-factor test (Podsakoff et al. 2003) and the marker variable test (Lindell and Whitney 2001). Both tests indicate that common method bias was not a threat to the validity of the study.

**Figure 2: Research Model and Results**

<table>
<thead>
<tr>
<th>General motivation</th>
<th>Situational motivation</th>
<th>Control Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal PLOC</td>
<td>Self-Efficacy</td>
<td>Age, Gender, Years of work-experience, Company Size, IT Job Function, Industry</td>
</tr>
<tr>
<td>H6: .379**</td>
<td>H2: .084**</td>
<td>R² = .520</td>
</tr>
<tr>
<td>H5: .600**</td>
<td></td>
<td>* p &lt; 0.05</td>
</tr>
<tr>
<td>H8: .067**</td>
<td>H4: .355**</td>
<td>** p &lt; 0.001</td>
</tr>
<tr>
<td>H7: -.007</td>
<td>H1: .242**</td>
<td>PLOC = Perceived Locus of Causality</td>
</tr>
<tr>
<td>External PLOC</td>
<td>Attitude</td>
<td></td>
</tr>
<tr>
<td></td>
<td>H3: .266**</td>
<td></td>
</tr>
</tbody>
</table>

**Discussion and Implications**

The goal of this study was to develop and test a comprehensive model of employees’ endogenous motivations to comply with organizational ISPs. Understanding which factors motivate ISP compliance behavior is crucial as employees’ compliance behavior has been found to be one of the most important determinants of successful ISS management (Ernst and Young 2005, Siponen and Vance 2010). Since prior research has neglected the important role of endogenous motivation and the internalization of ISPs, our study addressed this important gap in the IS security literature and provides valuable insight both for practitioners and scholars alike. We developed and empirically tested a model that examined how TPB's situational constructs are influenced by contextual endogenous motivations represented by the SDT/OIT. Integrating the TPB and SDT/OIT augments our understanding of the underlying motivational processes of ISP compliant behavior beyond the classical carrot and stick approach. We tested the model with survey data from 444 employees. In general, we find strong empirical support for the model, explaining a substantial proportion of the variance in ISP compliance intention (R² = .52).

In particular, the results provide strong empirical evidence that employees who perceive their behavior as self-determined and internalize ISS management's external regulations are more likely to comply with ISPs. In contrast, external PLOC had no impact on the intention to comply implying that the effectiveness of traditional approaches based on deterrence or remuneration mechanisms are limited. Hence, employees who perceive the regulations prescribed in the ISP as congruent with their own values, have a significantly higher intention to comply with the ISP. Our findings underscore the importance of establishing an organizational ISS-aware culture (Haeussinger and Kranz 2013) that not only focuses on how employees should behave, but also why doing so is important for employees, the organization and its customers and suppliers. The combination of the TPB and the SDT/OIT confirms the hypothesis that general motivations at the contextual level (internal and external PLOC) strongly impact TPB’s belief-based constructs at the situational level (Vallerand 1997, 2000), which significantly influence compliance intention. The integration of both theories particularly highlights the essential role of internal PLOC, since
beyond its strong direct effect it also has an indirect effect on intention through attitude and self-efficacy. The relationship between external PLOC and attitude in contrast was only moderate showing that employees’ evaluations of the advantageousness of ISP compliant behavior are less dependent on external regulation than on personal motives and internalized values. Our findings suggest that while deterrence mechanisms surely remain important, they do not suffice to motivate employees’ commitment in establishing ISS.

From a practitioners’ point of view, the crucial challenge in aligning employees’ ISS-related behavior with a company’s ISP requirements is to shift their perceived locus of causality from external to internal. Therefore, ISS practitioners should stimulate the internalization of security regulations. One step in this direction is to avoid presenting ISPs to employees without sufficiently explaining why those are critical for the company and even the smallest misconduct can have severe consequences. Further, security trainings should be designed to substantiate and explain the importance of security regulations so that employees understand that their individual behavior can put them as well as their organization and customers at risk to mitigate personal indifference. To avoid feelings of coercion it should be made clear that ISPs do not exist to patronize employees and each rule has its goal. ISPs should further be aligned to general interests of employees such as having a secure job. The importance of internal PLOC and the weak influence of external PLOC also imply that deterrence-based mechanisms like monitoring or punishment can only complement an effective security management. In this respect, Siponen (2000) noted that the process of internalizing ISS regulations does not arise from itself, but is built on a long-term foundation of general awareness and specific ISP knowledge. Hence, security managers should also focus on information security awareness building/maintaining levers. Since there is no reason to belief that irregular trainings will lead to employee’s internalization of the ISP, it is crucial to regard raising awareness as a gradual process and long-term goal (Siponen 2000, Haeussinger and Kranz 2013).

The study has some limitations that should be considered when interpreting the results. First, the data collection procedure was geographically confined to Western Europe. Hence, to generalize the findings future research is needed to account for cultural differences, which may be of particular interest for multinational organizations. Second, the cross-sectional design of the data limits the generalizability of the findings in at least two ways: With regard to information security, user perceptions may change significantly over time, e.g. because of contemporary incidents. Also the posited causal relationships can only be inferred. Thus, we encourage future research to employ longitudinal research designs. Other limitations are due to restrictions of the measurement instrument.

First, we had to rely on intention to comply as dependent variable instead of actual behavior. Although there exists empirical support that employee’s intention to comply with ISPs are significantly correlated with actual compliance behavior (e.g. Pahnila et al. 2007a), future research is needed to confirm the findings. Second, for our dependent variable “intention to comply” we used what Siponen and Vance (2014) call a generic measure. They argue that measurements of policy compliance intentions are more accurate if instrumentation includes contextualized examples of ISP compliance (Siponen and Vance 2014). Future research should address this limitation by applying more specific measures. Third, our applied operationalizations of IPLOC and EPLOC do not accurately reflect the PLOC continuum but rather represent the end points of the continuum. Therefore we suggest that future research should use a relative measure of PLOC, e.g. following Hagger et al. (2006).

Conclusion

A key goal of research on IS security is to identify and understand how managerially controllable antecedents influence employees’ information security policy (ISP) compliance behavior. Our study provides important insights into the role of endogenous motivations guiding employees’ intention to comply with their organization’s ISPs. By disentangling extrinsic and intrinsic motivations our research provides new evidence on how ISP compliance is influenced by different endogenous psychological states and reveals insights why deterrence is not enough. Our study refines prior research, provides essential implications for practitioners and researcher, and serves as a starting point for further research into the role of users’ endogenous motivations and values on ISS behavior. From a practitioners’ point of view the model can help to identify effective strategies to address and encourage employees to follow ISPs by increasing endogenous motivations. Such strategies are expected to lead to a more persistent and superior behavioral performance (Deci and Ryan 2002).
References


