Understanding the Antecedents of Information Security Awareness - An Empirical Study

Completed Research Paper

Haeussinger, Felix
Georg-August University of Göttingen
felix.haeussinger@googlemail.com

Kranz, Johann
Georg-August University of Göttingen
jkranz@uni-goettingen.de

ABSTRACT
Employees’ information security awareness (ISA) is a key antecedent of information security behavior. However, to date we know very little about the factors that are responsible for some employees having a higher level of ISA than others. Our study addresses this gap. We propose a model that comprises institutional, individual, and environmental factors preceding ISA. The model was empirically tested with survey data gathered from 475 employees of different organizations and industries. The model was found to explain a substantial proportion (.53) of the variance. The results indicate that providing employees with comprehensible and readily accessible information on security policies and improving employees’ IT knowledge are the two most influential antecedents of ISA. The findings will help refining researchers’ understanding of ISA and will be useful for diverse stakeholders interested in encouraging employees’ information security policy compliant behavior.

Keywords

INTRODUCTION
Violations of information security are a major challenge for organizations worldwide and are responsible for enormous economic damages each year (United Nations 2005, D’Arcy, Hovav, and Galletta 2009). The vast and increasing importance of information security has attracted scholars and security managers to investigate how information systems security (ISS) threats can be reduced effectively. Prior research on ISS was dominated by technological issues (e.g. encryption technology, spyware-detection, virus-detection, firewalls, etc.) (Spears and Barki 2010). However, it is assumed that 50 – 70 % of overall ISS incidents in organizations result either directly or indirectly from employees’ misuse – ranging from naïve mistakes to intentional destruction (Ernst and Young 2003, Siponen and Vance 2010). Against this background many recent studies investigated the role of employees’ ISA. Research found that ISA is a core antecedent of security behavior which is conceptualized either as information system (IS) policy compliance (e.g., Bulgurcu, Cavusoglu, and Benbasat 2010) or as IS misuse behavior (e.g., D’Arcy et al. 2009). Also managers claim that establishing ISA is one of the most important issues of security management (Tsouh, Kokolakis, Karyda, and Kiountouzis 2008). In this regard security management refers to making employees aware of their behaviors’ potential security risks and qualify them to use organizational IS resources responsibly (NIST 2003). Although ISA’s important role is widely recognized our understanding as to the factors influencing ISA is scarce. Hence, in a special issue of the MIS Quarterly Bulgurcu et al. (2010) state that “identifying the factors that lead to information security awareness would be an important contribution to academics, since there is a gap in the literature in this direction, as well as to practitioners, since they can use these factors to formulate their information security awareness programs.” Our study aims at addressing this gap.

The remainder of the paper is structured in six sections. In the following paragraph, we review prior research on information security awareness and elaborate on the theoretical background. In section 3 the research model is presented and the study’s hypotheses are derived. We then outline the methodology (section 4) and present the results (section 5). The paper concludes with a discussion of the results and provides implications for research and practice (section 6).

THEORETICAL BACKGROUND
Because of the socially constructed nature of ISA no universal definition exists in the literature (Tsouh et al. 2008). By carefully reviewing the IS literature, we identified three different perspectives on ISA, those are “procedural”, “behavioral”, and “cognitive”. From a process perspective the methods and different developmental phases of ISA such as the planning and
execution of awareness raising initiatives are at the core (e.g., NIST 2003). The behavioral perspective puts emphasis on behavioral dimensions affecting ISA such as the employee's intention of acting responsibly or conforming to IS policies. These actions range from "being committed to information security" (Rezgui and Marks 2008) to "help [...] effectively protect the organization's information assets" (Rotvold 2008). Most commonly ISA is studied from a cognitive perspective. ISA is then defined as an employee’s state of mind, which is characterized by recognizing the importance of IS security objectives, risks and threats, and having the required knowledge to use IS responsibly (Straub and Welke 1998, Thomson and von Solms, 1998, Siponen 2000). Although in line with this view, Bulgurcu et al. (2010) differentiate between the two ISA dimensions “General Information Security Awareness” (GISA) and “Information Security Policy Awareness” (ISPA). GISA corresponds to an individual’s overall knowledge and understanding of ISS issues and their potential consequences, while ISPA refers to the knowledge and understanding of the requirements of the organization’s ISPs. Since the aim of our paper is to identify the antecedents of both dimensions comprised in ISA, we conceptualize ISA as a second order construct following Bulgurcu et al. (2010).

ANTECEDENTS OF INFORMATION SECURITY AWARENESS

To capture the different facets influencing ISA our proposed research model (see figure 1) incorporates variables related to ISS management practices, and social psychology to address individual and social aspects. Thus, we categorized the antecedents of ISA into the dimensions institutional, individual, and environmental.

Figure 1: Research Model

Institutional Antecedents

Institutional antecedents refer to an organization’s security management practices. In the IS literature these factors are often summarized under the term “management support” (Chan, Woon, and Kankanhalli 2005). The higher the management support, the more resources for security issues are available (Herath and Rao 2009b). Scholars have emphasized that reasonable resources for security management are essential for establishing a sufficient level of security awareness among employees (Tsouhou, Karya, Kokolakis, and Kiountouzis 2010). Reviewing the IS literature, we identified security education training awareness (SETA) programs and information security policy the provision (ISPP) as important institutional antecedents of ISA.
Information Security Policy Provision

The development, transparency, and availability of corporate information security policies (ISPs) are primary resources of ISS management practices (Chan, Woon, and Kankanhalli et al. 2005). An ISP can be broadly defined as statements from an organization which provide guidance about ISS related responsibilities, rules, and guidelines which prescribe how the IS resources are used properly and in a secure way (D’Arcy et al. 2009). Prior research offers contradicting results with regard to the effect of ISPs. While D’Arcy et al. (2009) found corporate ISPs to be effective for preventing IS-misuse behavior and ascribe this effect to deterrence mechanisms, Lee, Lee, and Yoo (2004) found that the existence of an ISP had no influence on misuse behavior. Literature argues that this is a result of employees’ lack of awareness of security policies (Thomson and von Solms 1998, Siponen 2000).

In this respect, research found that ISPs which are made easily accessible on- and offline and are written in a clear and understandable way lead to policy compliant behavior (Chan et al. 2005, Herath and Rao (2009b). However, none of these studies incorporated ISA. We hypothesize that the reported positive effects of ISP provision on security behavior result at least partially from an increase in employees’ ISA. Based on the definition of ISA we claim that the reported positive direct effects of ISP on behavioral intention are largely a result of an increase in the employees’ awareness regarding ISP and therefore also of security issues in general. Our rationale is that promoting easily accessible and comprehensible ISPs raise employees’ contextual awareness and knowledge in the first place. Thus, in line with the suggestion of Siponen, Mahmood, and Pahnila (2009) we contend that the provision of easily understandable and accessible ISPs is positively related to employees’ ISA.

**Hypothesis 1:** ISP provision in the sense of providing easily comprehensible and accessible ISPs positively influences employees’ level of ISA.

SETA Programs

Mostly institutional security training activities are related to security education, security training, and awareness raising programs (Crossler and Bélanger 2006) typically referred to as SETA programs (D’Arcy et al. 2009). These programs aim to improve ISS by increasing employees’ knowledge and awareness of potential security risks, policies, and responsibilities (Straub and Welke 1998, Lee and Lee 2002, D’Arcy et al. 2009). Thus, SETA programs are regarded as critical to ensure a sufficient level of ISA among employees as they make employees aware and knowledgeable about organizations’ vulnerabilities to security threats (Siponen et al. 2009). Thus, we state:

**Hypothesis 2:** The existence of SETA programs in organizations positively influences employees’ level of ISA.

Individual Antecedents

The IS security literature regularly found that individual attitudes, knowledge, and experiences influence ISS compliant behavior (Rhee, Kim, and Ryu 2009, Bulgurcu et al. 2010). Reviewing prior research we identified two individual antecedents, which are hypothesized to have a direct effect on ISA through its GISA and ISPA dimensions.

**IT Knowledge**

Our study refers to IT knowledge as general knowledge of the basic IT applications used in daily business, such as computers, email systems, and the internet. Research implicates that there is a positive relationship between computer skills and awareness of ISS related issues (Frank, Shamir, and Briggs 1991) and the usage of ISS technology (Dinev and Hu 2007). Thus, we expect that IT knowledgeable individuals are more aware of IS security related threats and potential risks. Hence, we contend:

**Hypothesis 3:** The level of general IT Knowledge positively influences employees’ level of ISA.

**Negative Experience**

Employees may have directly or indirectly been harmed by any kind of IS security incidents such as worms, viruses, or phishing attacks either in private or working contexts. These experiences “such as having once been harmed by a virus attack or penalized for not adhering to security rules and regulations” (Bulgurcu et al. 2010) are likely to increase an individual’s ISA. Therefore, we hypothesize that individuals having been negatively affected by ISS incidents either directly or indirectly are more aware of information security.

**Hypothesis 4:** Negative experiences with ISS incidents positively influence employees’ level of ISA.
Environmental Antecedents

Theories in behavioral research (Fishbein and Ajzen 1975) and social psychology (Fulk, Steinfield, and Power 1987) highlight that individual behavior is always embedded in situational contexts and is thus susceptible to interactions with one’s social environment. The social environment can be separated in primary sources’ influence of close peers such as family members, friends, or co-workers and secondary sources such as mass media (e.g., Brown and Venkatesh 2005).

Secondary Sources’ Influence

Several studies in the ISS domain suggest that individuals’ understanding of security threats and their security behavior are positively related to information received from mass media including newspapers, radio, internet, and TV (Herath and Rao, 2009b, Siponen et al. 2009, NG and Rahim 2005). As Furnell (2006) emphasizes information related to ISS in the mass media can have an impact on the public awareness towards information security matters. The positive impact of mass media coverage about security threats on individual knowledge and behavior is assumingly largely due to an increase in the recipients’ level of ISA. Accordingly, Bulgurcu et al. (2010) state that employees’ ISA may be a result of information from external sources. Hence, we contend that information received from secondary sources highlighting potential risks and the importance of information security positively impacts ISA.

Hypothesis 5: Information about ISS from secondary sources positively influences employees’ level of ISA.

Peer Behavior

In the context of ISS empirical evidence shows the positive impact of ISP-compliant behavior of peers on the security behavior of others (Herath and Rao (2009a). It has also been shown that direct supervisory security practices and direct co-workers socialization, including conversations, observing behavior of co-workers and the consequences of certain behaviors increase an employee’s perception of ISPs which positively affects security compliant behavior (Chan et al. 2005). Moreover, if co-workers disapprove the ISP violations employees are found to be less likely to do so (Siponen and Vance 2010). Also in the private context it could be empirically proven that family members and peers significantly affect an user’s intention to behave responsible with regard to computer security (NG and Rahim 2005). Thus there is strong evidence that peers affect employees’ security behavior. Interactions with peers enable knowledge transfer (Spears 2006) and increasing ISS knowledge goes hand in hand with increasing ISA because of ISA’s knowledge dimension. Leach (2003) accordingly states that the security behavior of co-workers has an impact on employee’s ISA. Following this rationale, we state:

Hypothesis 6: ISP compliant peer behavior positively influences employees’ level of ISA.

RESEARCH METHODOLOGY

Sample and data-collection procedure

To test our model we conducted an online survey in October 2012. 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 1,120 initial visitors 661 finished the questionnaire completely. From this sample we excluded respondents who were self-employed (n = 65) and whose firms did not have explicit ISPs (n = 59). A rough examination of the plausibility of several response schemes resulted in an elimination of further 24 cases. Additionally, we eliminated questionnaires with questionably short handling time (n = 38), resulting in a final sample size of n = 475. From this sample 68 % were female, and the average age was 35.3 years, ranging from 20 to 67 years. 81.3 % of the respondents held at least a college or university degree. The average work-experience was 10.8 years. 26 % percent of the participants worked for companies in the IT-industry, followed by “manufacturing” (9.7 %), “service industry” (9.3 %), “education and research” (8.6 %), and “consulting” (8.4 %). The sample was fairly evenly distributed concerning the different functions and positions of employees and company size - ranging from less than 100 to more than 10.000 employees.

Measurement of Constructs

We employed standard psychometric scale development procedures. Aside from the items of negative experience the items were assessed on seven-point Likert-scales ranging from strongly disagree (1) to strongly agree (7). We applied validated scales when possible, but adapted two measures, IT Knowledge and ISP Provision, to the context of our study. To validate these measures we conducted qualitative and quantitative pilot studies including sorting procedures with subsequent interviews of four practitioners and six scholars (Moore and Benbasat 1991). The dependent variable “ISA” was operationalized as second-order construct, composed of the two first-order constructs “General ISA” and “ISP Awareness” (Bulgurcu et al. 2010). Based on the feedback of two pre-tests (n = 25) the wording and order of some items were revised. The final items of the latent variables along with the psychometric properties are outlined in table 1.
### Table 1: Measurement instrument and factor loadings

<table>
<thead>
<tr>
<th>Construct (Source)</th>
<th>Items</th>
<th>Type</th>
<th>Factor Loading</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Information Security Awareness</strong> (Bulgurcu et al. 2010)</td>
<td>Overall, I am aware of the potential security threats and their negative consequences.</td>
<td>reflective</td>
<td>.897***</td>
</tr>
<tr>
<td></td>
<td>I have sufficient knowledge about the cost of potential security problems.</td>
<td>reflective</td>
<td>.772***</td>
</tr>
<tr>
<td></td>
<td>I understand the concerns regarding information security and the risks they pose in general.</td>
<td>reflective</td>
<td>.820***</td>
</tr>
<tr>
<td><strong>Information Security Policy Awareness</strong> (Bulgurcu et al. 2010)</td>
<td>I know the rules and regulations prescribed by the ISP of my organization.</td>
<td>reflective</td>
<td>.935***</td>
</tr>
<tr>
<td></td>
<td>I understand the rules and regulations prescribed by the ISP of my organization.</td>
<td>reflective</td>
<td>.903***</td>
</tr>
<tr>
<td></td>
<td>I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization.</td>
<td>reflective</td>
<td>.931***</td>
</tr>
<tr>
<td><strong>Information Security Policy Provision</strong> (Herath and Rao 2009b, Chan et al. 2005)</td>
<td>Information security policies are written in a manner that is clear and understandable.</td>
<td>formative</td>
<td>.611***</td>
</tr>
<tr>
<td></td>
<td>Corporate information security policies are readily available for my reference.</td>
<td>formative</td>
<td>.479***</td>
</tr>
<tr>
<td><strong>SETA Programs</strong> (D’Arcy et al. 2009)</td>
<td>In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.</td>
<td>formative</td>
<td>.531***</td>
</tr>
<tr>
<td></td>
<td>My organization educates employees on their computer security responsibilities.</td>
<td>formative</td>
<td>.282*</td>
</tr>
<tr>
<td></td>
<td>In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.</td>
<td>formative</td>
<td>.307**</td>
</tr>
<tr>
<td><strong>IT Knowledge</strong> (Bassellier et al. 2003)</td>
<td>What is your general knowledge of personal computer?</td>
<td>reflective</td>
<td>.914***</td>
</tr>
<tr>
<td></td>
<td>What is your general knowledge of Internet?</td>
<td>reflective</td>
<td>.924***</td>
</tr>
<tr>
<td></td>
<td>What is your general knowledge of email-systems?</td>
<td>reflective</td>
<td>.929***</td>
</tr>
<tr>
<td><strong>Negative Experience</strong> (Rhee et al. 2009)</td>
<td>Have you ever had problems because of a virus on your computer during the last two years?</td>
<td>reflective</td>
<td>.870***</td>
</tr>
<tr>
<td></td>
<td>Have you ever had spyware on your computer during the last two years?</td>
<td>reflective</td>
<td>.795***</td>
</tr>
<tr>
<td><strong>Secondary Sources’ Influence</strong> (Brown and Venkatesh 2005)</td>
<td>Information from mass media (TV, radio, newspapers, internet) suggest that I should comply with the information security policy of my employer.</td>
<td>reflective</td>
<td>.844***</td>
</tr>
<tr>
<td></td>
<td>Information that I gather by mass media (TV, radio, newspapers, internet) encourage me to comply with the information security policy of my employer.</td>
<td>reflective</td>
<td>.958***</td>
</tr>
<tr>
<td></td>
<td>Based on what I have heard or seen on mass media (TV, radio, newspapers, internet), I am encouraged to follow the information security policy of my employer.</td>
<td>reflective</td>
<td>.957***</td>
</tr>
<tr>
<td><strong>Peer Behavior</strong> (Herath and Rao 2009a)</td>
<td>I believe other employees comply with the organization IS security policies.</td>
<td>reflective</td>
<td>.951***</td>
</tr>
<tr>
<td></td>
<td>I am convinced other employees comply with the organization IS security policies.</td>
<td>reflective</td>
<td>.918***</td>
</tr>
<tr>
<td></td>
<td>It is likely that the majority of other employees comply with the organization IS security policies to help protect organization's information systems.</td>
<td>reflective</td>
<td>.909***</td>
</tr>
</tbody>
</table>

* p < .05; ** p < .01; *** p < .001;

The study incorporates reflective and formative measurement scales. The variables ISP Provision and SETA programs were modeled as formative measures based on the criteria specified by Jarvis, Mackenzie, and Podsakoff (2003). The other variables of the study were modeled as reflective constructs. Since formative constructs cannot be assessed by the same
reliability and validity tests as reflective constructs, we assessed them separately (Diamantopoulos and Winklhofer 2001). To assess the reflective variables we assessed reliability and validity according to the guidelines of Gefen and Straub (2005).

As illustrated in table 1 all reflective items loaded significantly on the underlying constructs with values well above the recommended threshold of .707 (Chin 1998). Composite reliability (CR) scores also exceed the recommended threshold of .70 (Gefen and Straub 2005) (see table 2). Furthermore, we carried out a confirmatory factor analysis and checked cross-loadings. All indicator items loaded more strongly on their corresponding construct than on any other construct. Hence, reliability tests indicated that indicator and construct reliability was well developed. Convergent validity was assessed by examining the constructs’ average variance extracted (AVE). Results indicate that the average variance explained of each construct was well above the common threshold of .50 (Bhattacherjee and Premkumar 2004). To establish discriminant validity the criterion of Fornell and Larcker (1981) was applied. As the squared correlations between any two constructs are lower than the corresponding AVE discriminant validity is established.

Table 2: Reflective Measure Validation: Composite Reliability, AVE, Latent Variable Correlation

<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>GISA</th>
<th>ISPA</th>
<th>NEX</th>
<th>ITK</th>
<th>SSI</th>
<th>PEB</th>
</tr>
</thead>
<tbody>
<tr>
<td>GISA</td>
<td>1-7</td>
<td>5.56</td>
<td>1.12</td>
<td>.870</td>
<td>.774</td>
<td>.691</td>
<td>.831</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISPA</td>
<td>1-7</td>
<td>5.48</td>
<td>1.32</td>
<td>.946</td>
<td>.913</td>
<td>.853</td>
<td>.593</td>
<td>.924</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEX</td>
<td>1-2</td>
<td>1.28</td>
<td>.37</td>
<td>.820</td>
<td>.565</td>
<td>.695</td>
<td>.030</td>
<td>.035</td>
<td>.834</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITK</td>
<td>1-7</td>
<td>5.48</td>
<td>1.32</td>
<td>.945</td>
<td>.913</td>
<td>.851</td>
<td>.377</td>
<td>.320</td>
<td>-.072</td>
<td>.922</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSI</td>
<td>1-7</td>
<td>4.67</td>
<td>1.62</td>
<td>.944</td>
<td>.914</td>
<td>.848</td>
<td>.283</td>
<td>.227</td>
<td>-.023</td>
<td>-.028</td>
<td>.921</td>
<td></td>
</tr>
<tr>
<td>PEB</td>
<td>1-7</td>
<td>4.78</td>
<td>1.44</td>
<td>.947</td>
<td>.917</td>
<td>.857</td>
<td>.272</td>
<td>.416</td>
<td>-.103</td>
<td>.016</td>
<td>.287</td>
<td>.926</td>
</tr>
</tbody>
</table>

Note. CR = Composite Reliability; AVE = Average Variance Extracted, CA = Cronbach Alpha; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; NEX = Negative Experience; ITK = IT Knowledge; SSI = Secondary Sources’ Influence; PEB = Peer Behavior; bold diagonal elements represent the square-root of AVE; CA, CR, AVE cannot be computed for formative measures.

To verify the validity of the two formative constructs (SETA programs: mean = 4.24, SD = 1.87 and ISPP: mean = 5.21, SD = 1.53), we calculated indicator weights (Petter, Straub and Rai, 2007). The formative indicators were significant p < 0.01 and exceeded the threshold of 0.20, indicating good construct validity (Chin 1998). To examine convergent and discriminant validity of the remaining formative indicators, a “weighted” item-to-construct matrix was created (Loch, Straub, Kamel 2003). Convergent validity could be established as all indicators significantly correlated with their corresponding construct. Also each indicator’s weighted score correlates higher with its own construct than with the composite score of any other formative construct, indicating sound discriminant validity (Loch et al. 2003). To evaluate the reliability of the formative constructs, we tested for multicollinearity (Diamantopoulos and Winklhofer 2001). The variance inflation factors (VIF) ranged from 1.72 to 3.80, thus indicating satisfactory reliability (Hair et al. 1998).

RESULTS

The research model was validated using structural equation modeling. In particular, we applied the component-based partial least square (PLS) approach using SmartPLS version 2.0.M3 (Ringle Wende, and Will 2005). The PLS method was chosen because of its ability to handle reflective and formative measurement scales both used in this study (Jarvis et al. 2003). The significance of the parameter estimates was calculated applying bootstrapping with 3,000 samples. The results show (see figure 2) that all hypotheses are supported (p < .05). The research model could explain .53 of the variance of the dependent variable ISA. The weights of the two sub-dimensions GISA (w₁ = .48) and ISPA (w₂ = .64) of the second order construct ISA were also significant (p < .001), indicating that each sub-dimension significantly contributes to the underlying overall factor (Bulgurcu et al. 2010). We also tested for common method bias as independent and dependent variables were provided by the same respondent. Both, the Harman’s single-factor test ( Podsakoff, MacKenzie, Lee, and Podsakoff 2003) and the marker variable test (Lindell and Whitney 2001) indicate that common method bias is not a threat to the validity of our study.
**DISCUSSION AND IMPLICATIONS**

Our study addressed an important gap in ISS literature regarding the emergence of employees’ ISA. Understanding which factors influence ISA is crucial as employees’ awareness has been found to be a substantial determinant of ISS compliant behavior. In our study we proposed and empirically tested a research model comprising institutional, individual and environmental antecedents. The model received ample support ($R^2 = .53$) and provides important implications for ISS management practices. The findings imply that the provision of ISPs to employees is the single most substantial antecedent of ISA. Thus, an effective and relatively easy way to make employees aware of information security issues is to provide policies which are understandable for all employees of an organization and easily accessible on- and offline at any time.

Although many scholars claim that SETA programs increase ISA, hitherto empirical evidence was limited. Our results confirm the hypothesized positive effect of security trainings on ISA. Thus, an essential task of security and general management is to provide employees with suitable SETA programs. On the individual level, we found that general IT-knowledge is an essential predictor of ISA. The more employees know about IS and IT the more knowledgeable and aware they are regarding ISS related issues. Therefore, organizations should seek to improve the IT skills of those employees lacking general IT knowledge to avoid unintentional misbehavior. Prior negative experiences with ISS incidents also had a positive - although smaller - effect on ISA supporting the rationale that once being affected by incidents increases individual awareness of ISS issues. Therefore, to increase ISA and consequently ISP compliant behavior of employees, organizations may build on this finding by offering information on attempted and actual cyber-attacks on the organization to point out the virulent threats of misbehavior. Also information about IS security incidents from outside the organization should be communicated as the study found that information provided by secondary sources also raises ISA. The same effect was found for the influence of peer behavior, however to a lesser extent. This finding was unexpected as prior research suggests that the behavior of peers is an important antecedent of ISA. One reason for this might be that the ISS compliant behavior of peers is difficult to observe and thus does not affect the individual ISA as strong as the literature would suggest.

As with any other empirical study this study has limitations that should be considered when interpreting the results. The data collection procedure was geographically confined. Hence, to generalize the findings future research is needed to account for cultural differences which may be of particular interest for multinational organizations. Another limitation and also an avenue for further research is that due to time restrictions of the questionnaire we could not delve more deeply into the “black box” of SETA programs. Field experiments analyzing the security awareness of employees before and after SETA programs could substantially contribute to our understanding about the emergence of employees’ information security awareness.
REFERENCES


