# INFORMATION SECURITY AWARENESS: ITS ANTECEDENTS AND MEDIATING EFFECTS ON SECURITY COMPLIANT BEHAVIOR

*Completed Research Paper*

**Felix J. Haeussinger**
Georg-August-University Goettingen
Platz der Göttinger Sieben 5
37073 Goettingen
fhaeussinger@uni-goettingen.de

**Johann J. Kranz**
Georg-August-University Goettingen
Platz der Göttinger Sieben 5
37073 Goettingen
jkranz@uni-goettingen.de

## Abstract

*Information security awareness (ISA) is referred to as a state of consciousness and knowledge about security issues and is frequently found to impact security compliant behavior. However, to date we know little about the factors influencing ISA and its mediating effect on behavior. Our study addresses these gaps. We propose a research model that studies ISA's institutional, individual, and environmental antecedents and investigates the mediating role of ISA. The model was empirically tested with survey data from 475 employees. The model explains a substantial proportion of the variance of ISA (.50) and intention to comply (.41). The results imply that the provision of security policies and employees' knowledge on information systems are the most influential antecedents of ISA. The study shows that ISA mediates the relationship between ISA's antecedents and behavioral intention. The findings will be useful for stakeholders interested in encouraging employees' information security policy compliant behavior.*

**Keywords:** Information Security Awareness, Information Security Behavior, Information Security Training, Information Security Policy

# Introduction

Most organizations' functioning greatly relies on corporate information systems (IS). Thus, managing risk associated to security threats is getting increasingly important since violations of information security often have serious financial and reputational consequences for companies and their customers (Cavusoglu et al. 2004). Ensuring information security has become one of the major priorities and challenges for organizations. Consequently, academia and businesses are interested in how information system security (ISS) threats can be reduced effectively (D'Arcy et al. 2009). Although organizations spend evermore on technological solutions to safeguard information security, anecdotal and empirical evidence implies that the number and severity of incidents is growing (AIRC 2008; Symantec 2009). Similarly prior research on ISS was mainly focused on technological issues such as encryption technology, spyware and virus detection, or firewalls (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 harm (Ernst and Young 2003, Siponen and Vance 2010). Therefore, improving information security needs both investments in technical and socio-organizational resources (Bulgurcu et al. 2010). Against this background, recent studies shifted the focus on organizational, environmental, and individual factors that influence employees' behavior as they are regarded as the weakest link in information security (Siponen 2000, Boss et al. 2009, Bulgurcu et al. 2010). Prior research has found that increasing employees' information security awareness (ISA) has a strong positive effect on their ISP compliant behavior (Dinev and Hu 2007, D'Arcy et al. 2009, Bulgurcu et al. 2010). Also managers claim that establishing a sufficient level of ISA is one of the priorities of security management (Tsohou et al. 2008). In this regard security management refers to making employees aware of their behaviors' potential ramifications on information security 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 to add to the limited research on ISA and delves more deeply into Siponen's (2000) assertion that "ISA is one of the most important antecedents of behavior" by investigating the important, yet understudied, mediating role of ISA on the relation between ISA's antecedents and the intention to comply with the security policies. The remainder of the paper is structured in six sections. In the following paragraph, we review prior research on information security awareness and behavior 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 and Hypotheses Development

Owing to the socially constructed nature of ISA no universal definition exists in the literature (Tsohou et al. 2008). By carefully reviewing the IS literature, we identified three different perspectives on ISA, those are "procedural", "behavioral", and "cognitive". From a procedural 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 however, ISA is studied from a cognitive perspective, as done in this study. ISA is then defined as an employee's state of mind, which is characterized by recognizing the importance of ISS and being aware and conscious about IS security objectives, risks and threats, and having an interest in acquiring the required knowledge to use IS responsibly, if not already present (Siponen 2000; Straub and Welke 1998; Thomson and von Solms, 1998). Bulgurcu et al. (2010) additionally 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. Our study follows this notion and conceptualizes ISA as second order construct.

Diverse studies have proven ISA to be an important indirect and direct determinant of information security compliant behavior. For example, Galvez and Guzman (2009) identified ISA as one of the shaping factors of behavior and constitute that "the higher the information security awareness, the higher the information security practice". Dinev and Hu (2007) found that the user's awareness about potential risks and threats of harmful technologies is a determining factor of the intention to make use of protective information technologies. Applying the general deterrence theory, D'Arcy et al. (2009) showed that high level of employees' awareness on management's ISS countermeasures (Security Education Training Awareness (SETA) programs, computer surveillance, IS security policies) reduces the IT-misuse intention. Bulgurcu et al. (2010) studied the antecedents of employees' policy compliance investigating the role of ISA on the outcome beliefs (1) perceived benefit of compliance, (2) perceived cost of compliance and (3) perceived cost of noncompliance and attitude towards intention to comply. They found significant effects of ISA on the three outcome beliefs and attitude. Shedding a light on the mediating effect of attitude on the relationship between ISA and behavior, they found that attitude is only a partial mediator. Hence, we hypothesize a direct effect of ISA on the Intention to comply with security policies. Thus,

H1. ISA positively influences employees' Intention to comply with the ISPs.

## Antecedents of Information Security Awareness

To capture the different facets preceding ISA, our proposed research model (see figure 1) incorporates variables related to ISS management practices and social psychology to address individual, institutional and socio-environmental determinants of ISA.

### *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 et al. 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 sufficient levels of security awareness among employees (Tsohou et al. 2010). Reviewing the IS literature carefully we identified Security Education Training Awareness (SETA) Programs and Information Security Policy Provision (ISP Provision) as vital institutional factors that can have an impact on employees' ISA.

#### Information Security Policy Provision

The development of corporate information security policies (ISPs) is a primary resource of ISS management practices (Chan et al. 2005). An ISP can be broadly defined as statements by an organization providing 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 that the existence of corporate ISPs to be effective for preventing IS misuse behavior and ascribe this effect to deterrence mechanisms, Lee et al. (2004) found that ISPs had no influence on IS misuse behavior. Literature argues that the inconsistent results are due to employees' lack of awareness of security policies (Siponen 2000; Thomson and von Solms 1998). In this respect, scholars emphasize that the simple existence of ISPs is not enough and highlight the importance of promoting ISPs and ensuring that they are comprehensible, easily available, and understandable. We summarize these aspects of effectively promoting ISPs under the term ISP Provision. There is broad empirical evidence that ISP Provision is positively associated to the security related behavior (Chan et al. 2005). Also Siponen et al. (2009) found that the visibility of policies plays an important role on employees' compliance with organizational security policies. Herath and Rao (2009b) also showed that ISPs should be made easily

accessible and available to employees online and should be written in a clear and understandable way as this has positive effects on the Intention to comply. However, none of these studies investigated the effects of ISP Provision on ISA. Based on the definition of ISA we claim that the reported positive direct effects of ISP Provision on behavioral intention are largely a result of an increase in the employees' awareness regarding ISP and therefore of security issues in general. Our rationale is that promoting easily accessible and comprehensible ISPs firstly raise employees' contextual awareness and knowledge and secondly the situational intention to comply. Thus, we contend that ISA at least partially mediates the positive effect of ISP Provision on security compliant behavior. Hence,

H2a. ISP Provision positively influences employees' level of ISA.

H2b. ISA mediates the positive effects of ISP Provision on the Intentions to comply with ISP.

### SETA Programs

Institutional security training activities are related to security education, security training, and awareness raising programs typically referred to as SETA Programs (Crossler and Bélanger 2006; D'Arcy et al. 2009). SETA Programs aim to improve organizational information security by increasing employees' knowledge and awareness of potential security risks, policies, and responsibilities. Furthermore, they aim at providing employees with the skills necessary to comply with organizational ISS procedures (D'Arcy et al. 2009; Lee and Lee 2002; Straub and Welke 1998; Whitman et al. 2001).

Several studies provided evidence that SETA Programs are an essential building block of security management and that they influence information security behavior positively (Chan et al. 2005; Goodhue und Peltier 2002; Spionen 2000; Thomson and von Solms 1998). Scholars additionally emphasize the role of SETA Programs on employees' ISA (e.g., D'Arcy et al. 2009; Straub and Welke 1998). Siponen et al. (2009) state that security education helps employees to become aware and develop an interest in security issues. They also contend that SETA Programs raise employees' consciousness about the vulnerability of their organization owing to IS security threats. As the primarily goals of SETA Programs are on education, security training, and awareness, we contend that these programs have a positive impact on ISA and that the influence on Intention to comply is at least partially mediated by ISA. Thus,

H3a. The provision of SETA programs positively influences employees' level of ISA.

H3b. ISA mediates the positive effects of SETA programs on the Intentions to comply with ISPs.

## *Individual Antecedents*

### IS Knowledge

Our study refers to IS Knowledge as general knowledge of basic IS applications used in daily business. Research implicates that there is a positive relationship between computer skills and awareness of ISS related issues (Frank et al. 1991) and the usage of preventive ISS technology such as anti-spyware software (Dinev and Hu 2007). Gaston (1996) states that an organization's IT staff possesses more IS Knowledge than the employees in other departments and thus have a higher level of awareness of possible ISS risks. In a quantitative survey, Rhee et al. (2009) showed that the respondents' level of computer- and internet-related knowledge and experience had a positive impact on security behavior. We hypothesize that IS Knowledge affects awareness directly through its knowledge dimension and that the influence on Intention to comply is at least partially mediated by ISA. Thus,

H4a. IS knowledge positively influences employees' level of ISA.

H4b. ISA mediates the positive effects of general IS Knowledge on the Intentions to comply with ISPs.

### Negative Experience

Employees may have been harmed directly or indirectly by any kind of ISS incidents such as worms, viruses, or phishing attacks in private or working contexts. ISA may be shaped by such experiences as negative incidents raise the future consciousness and interest in how to prevent such incidents. Bulgurcu et al. (2010) accordingly state life experiences "such as having once been harmed by a virus attack or penalized for not adhering to security rules and regulations" may increase an individual's ISA. Therefore,

we hypothesize that individuals who have been negatively affected by ISS incidents either personally or indirectly are more aware of information security issues. We further claim that the expected positive impact of Negative Experiences on security behavior is compensated by the negative effect on actual security behavior arising from a perceived loss in the ability to ensure ISP compliant behavior due to Negative Experiences (Rhee et al. 2009). Hence, we only postulate the following hypothesis:

H5. 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 et al. 1987) highlight that individual behavior is always embedded in social 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 (Brown and Venkatesh 2005).

### Secondary Sources' Influence

Research has shown that information received from secondary sources such as media has an impact on individual behaviors (Ajzen 1985; Brown and Venkatesh 2005; Rogers 1995). Also several studies in the ISS domain suggest that individuals' understanding of security threats and their security behavior are positively related to information received from newspapers, journals, television, or the intra- or internet (Herath and Rao 2009b; NG and Rahim 2005; Siponen et al. 2009). Furnell (2006) contends that information related to ISS in media can have an impact on the public awareness towards information security issues. Bulgurcu et al. (2010) state that employees' ISA may be affected by information received from media. We argue that the positive impact of mass media coverage concerning ISS threats on recipients' ISA is largely due to an increased interest and knowledge on information security. The Theory of Planned Behavior (Ajzen 1991) argues that normative influences directly influence behavior. We hypothesize that given the effect of Secondary Sources' Influence on individual consciousness and knowledge the direct impact of secondary sources on Intention is at least partially mediated by ISA.

H6a. Information about ISS from secondary sources positively influences employees' level of ISA.

H6b. ISA mediates the positive effects of secondary sources' influence on the Intention to comply with ISPs.

### 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 and observing the behavior of co-workers increase an employee's attention for organizational ISPs, which in turn positively affects security compliant behavior (Chan et al. 2005). Moreover, if co-workers disapprove of 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 users' intention to behave responsible with regard to computer security (NG and Rahim 2005). Thus, there is strong evidence that peers affect employees' security behavior. However, we argue that interactions with peers initiate knowledge transfers (Spears 2006) and consequently increase ISS-related knowledge. Therefore, we contend that ISP compliant peer behavior firstly increases ISA through its knowledge dimension (Leach 2003) and the direct effect of peer behavior is at least partially mediated by ISA. Hence,

H7a. ISP compliant peer behavior positively influences employees' level of ISA.

H7b. ISA mediates the positive effects of ISP compliant peer behavior on the Intentions to comply with ISPs.

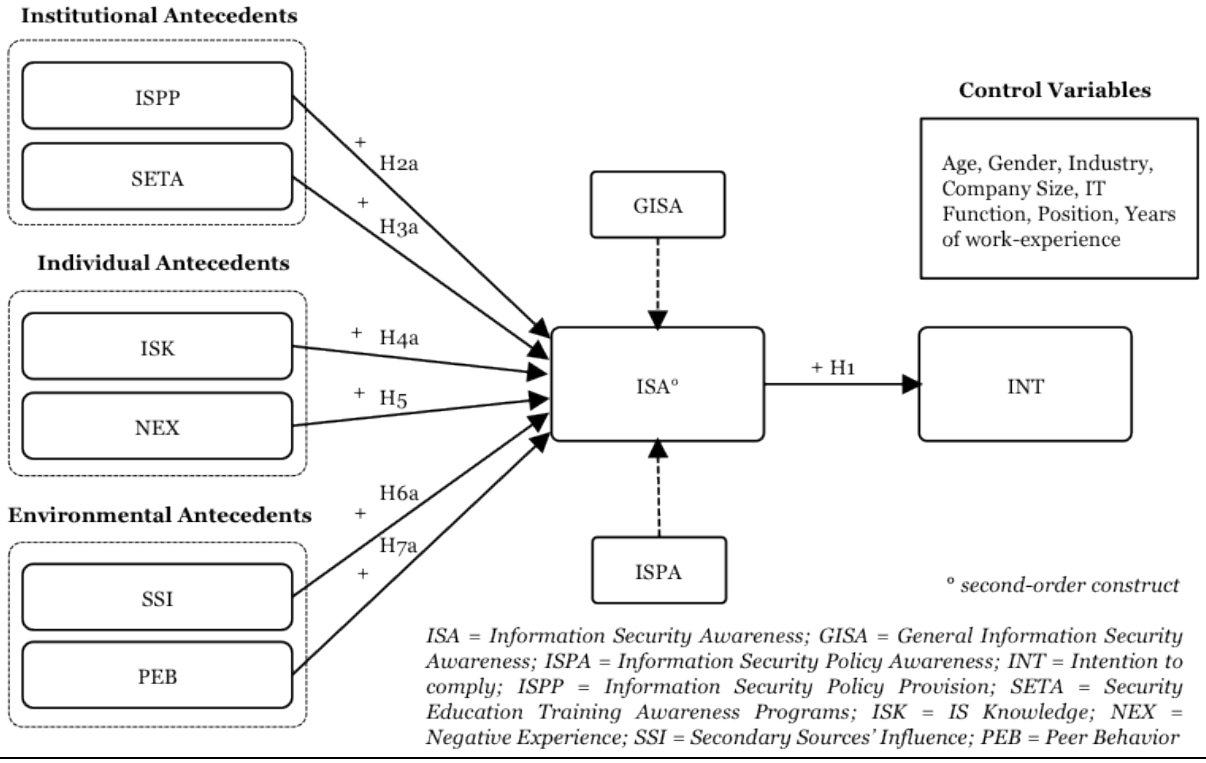


**Figure 1: Research Model**

# 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 1,120 initial visitors 661 finished the questionnaire completely. From this sample we eliminated questionnaires with implausible short handling time to avoid untrustworthy click-through answers (n = 38). We also excluded respondents who were self-employed (n = 65) and whose employer 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. The final sample size thus consists of 475 respondents. Sample demographics are summarized in Table 1.

| **Table 1: Demographics of Participants** | | |
|---|---|---|
| **Total Sample** | **n = 475** | |
| **Gender** | | |
| Male | 323 | 68.0% |
| Female | 152 | 32.0% |
| **Age** | | |
| 20-25 | 40 | 8.4% |
| 26-35 | 248 | 52.2% |
| 36-45 | 113 | 23.8% |
| 46-55 | 59 | 12.4% |
| 56-65 | 13 | 2.7% |
| 66 and over | 2 | 0.4% |
| **Industry** | | |
| Consulting | 40 | 8.4% |
| Education | 41 | 8.6% |
| Energy | 11 | 2.3% |
| Financial Services | 29 | 6.1% |
| Food and Beverages | 4 | 0.8% |
| Governmental | 16 | 3.4% |
| Hospital | 20 | 4.2% |
| IT and Telco | 123 | 25.9% |
| Manufacturing | 46 | 9.7% |
| Healthcare | 11 | 2.3% |
| Other services | 44 | 9.3% |
| Pharmacy and Chemistry | 11 | 2.3% |
| Real Estate Services | 2 | 0.4% |
| Wholesale / Retail | 18 | 3.8% |
| Others | 59 | 12.4% |
| **IT Function** | | |
| Yes | 77 | 16.2% |
| No | 398 | 83.8% |
| **Position** | | |
| Management | 146 | 30.7% |
| Office Worker | 221 | 46.5% |
| Technician | 108 | 22.7% |
| **Working Experience** | | |
| < 2 years | 66 | 13.9% |
| 3-5 years | 129 | 27.2% |
| 6-10 years | 96 | 20.2% |
| 11-15 years | 69 | 14.5% |
| 16-20 years | 36 | 7.6% |
| > 20 years | 79 | 16.6% |
| **Company Size** | | |
| < 100 employees | 87 | 18.3% |
| 100-499 | 112 | 23.6% |
| 500-999 | 31 | 6.5% |
| 1.000-2.499 | 42 | 8.8% |
| 2.500-9.999 | 70 | 14.7% |
| > 9.999 | 133 | 28.0% |

### *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 (GISA) and ISP Awareness (ISPA) (Bulgurcu et al. 2010). 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 (Bulgurcu et al. 2010). The variables ISP Provision and SETA Programs were modeled as formative measures based on the criteria specified by Jarvis et al. (2003). The other variables of the study were modeled as reflective constructs. 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 and the psychometric properties are depicted in table 2.

## Analysis and Results

The research model was validated using structural equation modeling. 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 of its ability to handle reflective and formative measurement scales both used in this study (Jarvis et al. 2003). Following the two-stage procedure proposed by Anderson and Gerbing (1988) we first assessed the psychometric properties of the measurement model and subsequently tested the hypotheses with the structural model.

### *Assessment of Measurement Model*

The study incorporates reflective and formative measurement scales. Since formative constructs cannot be assessed by the same reliability and validity tests as reflective constructs, we evaluated them separately (Diamantopoulos and Winklhofer 2001). To assess the reflective variables we conducted reliability and validity tests 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) and none of the items loaded on their construct below the cutoff value of .50. Composite reliability (CR) scores also exceeded the recommended threshold of .70 (Gefen and Straub 2005) (see table 3). 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. Hence, the tests imply that indicator and construct reliability was well developed. Convergent validity was assessed by examining the constructs' average variance extracted (AVE). Results indicate that the AVE 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 also established.

**Table 2: Measurement items and item loadings**

| Construct (Source) | Items | Scale | Type | Factor Loading |
|---|---|---|---|---|
| Intention to Comply (Bulgurcu et al. 2010) | 1_I intend to comply with the requirements of the ISP of my organization in the future. | a | r | .969*** |
| | 2_I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future. | a | r | .947*** |
| | 3_I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future. | a | r | .961*** |
| General Information Security Awareness (Bulgurcu et al. 2010) | 1_Overall, I am aware of the potential security threats and their negative consequences. | a | r | .896*** |
| | 2_I have sufficient knowledge about the cost of potential security problems. | a | r | .772*** |
| | 3_I understand the concerns regarding information security and the risks they pose in general. | a | r | .821*** |
| Information Security Policy Awareness (Bulgurcu et al. 2010) | 1_I know the rules and regulations prescribed by the ISP of my organization. | a | r | .935*** |
| | 2_I understand the rules and regulations prescribed by the ISP of my organization. | a | r | .903*** |
| | 3_I know my responsibilities as prescribed in the ISP to enhance the IS security of my organization. | a | r | .931*** |
| Information Security Policy Provision (Herath and Rao 2009b, Chan et al. 2005) | 1_Information Security policies are made available to employees online. | a | f | -.023† |
| | 2_Information security policies are written in a manner that is clear and understandable. | a | f | .652*** |
| | 3_Corporate information security policies are readily available for my reference. | a | f | .421*** |
| Security, Training and Awareness Programs (D'Arcy et al. 2009) | 1_My organization provides training to help employees improve their awareness of computer and information security issues. | a | f | -.031† |
| | 2_My organization provides employees with education on computer software copyright laws. | a | f | .155** |
| | 3_In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way. | a | f | .601*** |
| | 4_My organization educates employees on their computer security responsibilities. | a | f | .386*** |
| | 5_In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use. | a | f | .151 † |
| Information System Knowledge (adapted from Bassellier et al. 2003) | 1_What is your general knowledge of personal computers? | b | r | .910*** |
| | 2_What is your general knowledge of the internet? | b | r | .926*** |
| | 3_What is your general knowledge of email-systems? | b | r | .932*** |
| Negative Experience (Rhee et al. 2009) | 1_Have you ever had problems because of a virus on your computer during the last two years? | c | r | .872*** |
| | 2_Have you ever had spyware on your computer during the last two years? | c | r | .794*** |
| Secondary Sources' Influence (Brown and Venkatesh 2005) | 1_Information from mass media (TV, radio, newspapers, internet) suggest that I should comply with the information security policy of my employer. | a | r | .863*** |
| | 2_Information that I gather by mass media (TV, radio, newspapers, internet) encourage me to comply with the information security policy of my employer. | a | r | .954*** |
| | 3_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. | a | r | .949*** |
| Peer Behavior (Herath and Rao 2009a) | 1_I believe other employees comply with the organization IS security policies. | a | r | .949*** |
| | 2_I am convinced other employees comply with the organization IS security policies. | a | r | .919*** |
| | 3_It is likely that the majority of other employees comply with the organization IS security policies to help protect organization's information systems. | a | r | .910*** |

Note. * p < .05; ** p < .01; *** p < .001; † removed items; Scale a: Seven-point Likert scale: (1) "strongly disagree" –(7) "strongly agree"; Scale b: (1) "no general knowledge at all" – (7) "very good general knowledge"; Scale c: (1) = No; (2) = Yes; Type r = reflective; f = formative.

| **Table 3: Reflective Measure Validation: Composite Reliability, AVE, and Latent Variable Correlation** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Variable** | **Range** | **Mean** | **SD** | **CR** | **CA** | **AVE** | **INT** | **GISA** | **ISPA** | **NEX** | **ISK** | **SSI** | **PEB** |
| **INT** | 1-7 | 6.06 | 1.04 | 0.97 | 0.96 | 0.92 | **0.96** | | | | | | |
| **GISA** | 1-7 | 5.56 | 1.12 | 0.87 | 0.77 | 0.69 | 0.40 | **0.83** | | | | | |
| **ISPA** | 1-7 | 5.48 | 1.32 | 0.95 | 0.91 | 0.85 | 0.52 | 0.59 | **0.92** | | | | |
| **NEX** | 1-2 | 1.28 | 0.37 | 0.79 | 0.57 | 0.66 | -0.07 | 0.03 | 0.03 | **0.81** | | | |
| **ISK** | 1-7 | 5.48 | 1.32 | 0.94 | 0.91 | 0.85 | 0.16 | 0.38 | 0.32 | -0.71 | **0.92** | | |
| **SSI** | 1-7 | 4.67 | 1.62 | 0.95 | 0.91 | 0.85 | 0.35 | 0.28 | 0.22 | -0.09 | -0.31 | **0.92** | |
| **PEB** | 1-7 | 4.78 | 1.44 | 0.95 | 0.92 | 0.86 | 0.44 | 0.27 | 0.42 | -0.03 | 0.02 | 0.28 | **0.93** |

Note. CR = Composite Reliability; AVE = Average Variance Extracted, CA = Cronbach Alpha; INT = Intention to comply; GISA = General Information Security Awareness; ISPA = Information Security Policy Awareness; NEX = Negative Experience; ISK = IS 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 (ISP Provision: mean = 5.21, SD = 1.53; SETA programs: mean = 4.24, SD = 1.87), we calculated indicator weights (Petter et al. 2007). The formative indicator weights exceeded the threshold of .10 and were significant ($p < .01$) indicating good construct validity (Chin 1998). The item weights of "ISP Provision_1" (-.023) and "SETA_Programs_1" (-.031), "SETA_Programs_5" (0.151) were not significant. "ISP_Provision_1" and "SETA_Programs_1" were further under the threshold of 0.10. Literature suggests removing non-significant items from formative scales. Nevertheless, before removing items it should be considered whether the elimination would harm the content validity of the construct (Diamantopoulos and Winklhofer 2001). The three items were conceptualized more generally and therefore it could be assumed that an elimination of these items would not change the constructs' meanings. We tested the structural model twice with and without the removed items and found no significant differences in the results. For these reasons we decided to exclude „ISP_Provision_1" and "SETA_Programs_1", "SETA_Programs_5" from all following analyses.
To examine convergent and discriminant validity of the remaining formative indicators, a "weighted" item-to-construct matrix was created (Loch et al. 2003). Convergent validity could be established as all indicators significantly correlated with their corresponding construct. In addition, 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 und Winklhofer 2001). The variance inflation factors (VIF) ranged from 1.72 to 3.80 thus indicating satisfactory reliability (Hair et al. 1998).

## *Testing the Structural Model*

The research model was validated using structural equation modeling. The significance of the parameter estimates was calculated applying bootstrapping with 3,000 samples. The results show (see figure 2) that all hypothesized direct effects of ISA's antecedents on ISA are supported (H2a, H3a, H4a, H5, H6a and H7a ($p< .05$). Results also confirm the positive effect of employees' ISA on the Intention to comply with ISPs ($\beta = .30$, $p < .001$). The research model could explain for .50 of the variance in the variable ISA and for .40 of the variance in the variable Intention to comply. The weights of the two sub-dimensions GISA ($w_1 = .466$) and ISPA ($w_2 = .650$) of the second order construct ISA were also significant ($p < .001$) indicating that each sub-dimension significantly contributes to the underlying overall factor. None of the control variables except working experience ($\beta = .094$, $p<.05$) and gender ($\beta = -.137$, $p<.001$) were found to be significant. 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 et al. (2003) and the marker variable test (Lindell and Whitney 2001) indicate that common method bias was not a threat to the validity of our study.

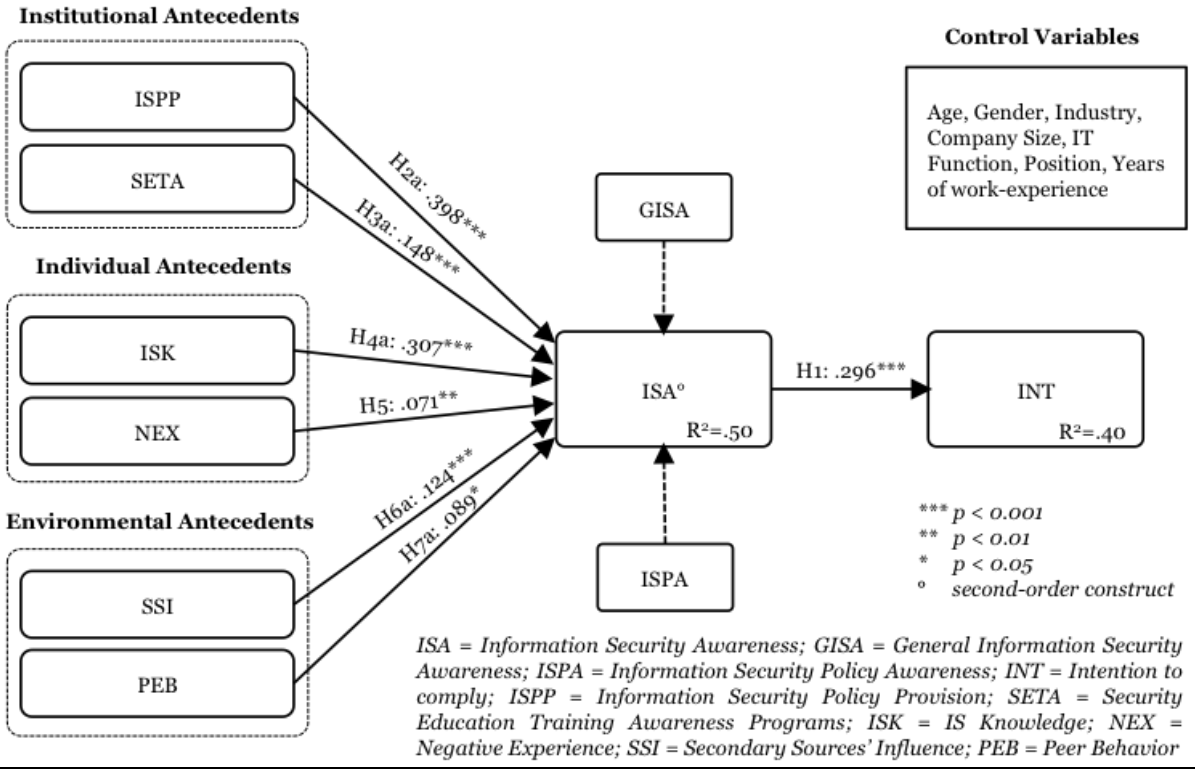


**Figure 2: Results**

## *Mediation Analyses*

To test the hypothesized mediating role of ISA we performed the widely used procedure proposed by Baron and Kenny (1986). The results of the mediation analysis are summarized in Table 4. For supporting significant mediation according to Baron and Kenny (1986) the following four conditions need to be fulfilled.

First, the independent variable (IV) must account for variations in the dependent variable (Intention to comply), when not controlling for the mediator (ISA) (path c'). This condition is successfully met for each IV ($p<.001$). Second, the mediator must significantly account for variations in the dependent variable (path b). This condition is likewise fulfilled ($ß = .296$, $p<.001$). Third, the IV must significantly account for variations in the mediator (path a). This condition is satisfied for all IV's with ($p<.001$) and Peer Behavior ($p<.05$). Finally, the effects of the IVs on the dependent variables (path c') must decrease significantly when controlling for the mediator (path c). The results suggest the existence of a full mediation, if path c' becomes statistically insignificant when controlling for the mediator (path c), and suggests a partial mediation, if path c' only decreases but path c still stays significant. Whether or not the mediation effect is significant can be examined by Sobel's (1982) test of indirect effects. It is tested whether the effects of the independent variable drops significantly once the mediator is incorporated into the model. The results in table 4 show that all mediation hypotheses were confirmed as all four conditions were met for each hypothesis. ISA fully mediates the effects of ISP Provision and SETA Programs on the Intention to comply and partially mediates the effects of IS Knowledge, Secondary Sources' Influence, and Peer Behavior.

| Table 4: Mediation Analyses of ISA | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Hypotheses** | **IV** | **Model II** | | | **Model I** | **Sobel's Test** | **Mediation** |
| | | **a** | **b** | **c** | **c'** | z | |
| H2b | ISPP | .398*** | .296*** | .055 | .166*** | 4.421*** | Full Mediation |
| H3b | SETA | .143*** | .296*** | .069 | .115*** | 2.639** | Full Mediation |
| H4b | ISK | .307*** | .296*** | .071* | .158*** | 4.24*** | Partially Mediation |
| H6b | SSI | .124*** | .296*** | .167*** | .203*** | 2.951** | Partially Mediation |
| H7b | PEB | .089* | .296*** | .212*** | .236*** | 2.069* | Partially Mediation |

Note. IV = Independent Variable; Model I: without controlling for the Mediator (ISA); Model II: with controlling for the Mediator; Path a: IV -> Mediator; Path b: Mediator -> Intention; Path c and c': IV-> Intention; * p < .05; ** p < .01; *** p < .001.

# Discussion and implications

Our study addresses an important gap in the information security 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 ISP compliant behavior. In the present study we proposed and empirically tested a research model comprising institutional, individual and environmental antecedents of ISA. The model explains a substantial proportion of the variance in ISA ($R^2$ = .50). The findings have important implications for information security managers and researchers. The promotion and provision of ISPs is the single most substantial antecedents of ISA. Thus, providing policies, which are understandable for all employees of an organization and easily accessible on- and offline at any time, are an effective, economic, and relatively easy way to make employees aware of information security issues. 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 IS Knowledge is an essential predictor of ISA. The more employees know about IS the more aware they are regarding ISS related issues. Therefore, organizations should seek to improve the skills of those employees lacking general IS 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 directly or indirectly by incidents the awareness of information security issues increases (Bulgurcu et al. 2010). To raise ISA 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 ISS 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. The significant effect of the control variables working experience and gender is also worth noting as they indicate that female employees and employees with greater working experience have a significantly higher Intention to comply with ISPs.

The mediation analysis reveals the significant role of ISA. ISA was found to fully mediate the relationships between Intention to comply and ISP Provision and SETA Programs. Additionally ISA partially mediates the effects of IS Knowledge, Secondary Sources' Influence, and Peer Behavior on Intention to comply. We can theorize about the reasons for the full mediating effect of ISA between ISP Provision and Intention and SETA Programs and Intention. ISA as defined by our study captures two dimensions, employees' general knowledge about information security and the cognizance of the employer's specific ISP. ISP Provision and SETA Programs address both dimensions and once ISA is established, the knowledge of general ISS-related issues and threats as well as an organization's ISP apparently become internalized by employees, hence a full mediation through ISA. These results underscore the vital role of employees' security awareness on security compliant behavior. ISA alone explains .40 of the variance in Intention to comply. Hence, security managers must stay focused on ISA-building/maintaining levers. In relation to the environmental variables (NEX, SSI, PEB) included in the research model, ISP Provision, SETA Programs, and IS Knowledge have a stronger impact on Intention through ISA. This is good news for ISS

managers as those variables can be influenced directly by organizations. Thus, the main resources of ISS managers should focus on an effective provisioning of comprehensible ISPs, offering target-group specific SETA Programs, and specifically addressing employee's IS skills shortage. Concentrating on those security countermeasures would also have a reinforcing effect on the relationships between normative influences (Secondary Sources' Influence and Peer Behavior) and Intention to comply, which are only partially mediated by ISA.

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 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. Further, we had to rely on Intention to comply as dependent variable instead of actual behavior. Although literature contends that intention is the most proximal influence on behavior it is not guaranteed that employees will behave as indicated. Although there exists sound empirical support that employee's intentions to comply with ISPs have a significant impact on actual compliant behavior (Pahnila et al. 2007), future research should reassess the research model measuring actual behavior. Another avenue for further research is to consider the effect of moral reasoning since an individual's moral commitment has been found to influence IS misuse intention (D'Arcy et al. 2009). Also future research could delve more deeply into the "black box" of SETA Programs. In this respect field experiments analyzing the security awareness of employees before and after SETA programs could substantially contribute to our understanding about the emergence of employees' ISA. Moreover, the cross-sectional design of the data limits the generalizability of our findings in at least two ways. First, with regard to information security, user perceptions may change significantly over time, e.g. because of contemporary incidents. Second, the posited causal relationships can only be inferred. Thus, we encourage future research to employ longitudinal research designs.

## Conclusion

A key goal of research on information security is to identify and understand how managerially controllable antecedents influence employees' security behavior. This article provides important insights on the antecedents of ISA and its mediating role on the relationship between its antecedents and Intention to comply with ISPs. Our results provide evidence that several institutional, individual, and environmental factors that prior research has considered as direct antecedents of security behavior are in fact at least partially mediated by ISA. Thus, our study refines prior research and serves as a starting point for further research on the role of ISA on security compliant behavior.

## REFERENCES

AIRC. 2008. Attack Intelligence Research Center Annual Threat Report: 2008 Overview and 2009 Predictions, *Attack Intelligence Research Center*, Alladin Knowledge Systems, Belcamp, MD (available online at http://www.aladdin.com/pdf/airc/ AIRC-Annual-Threat-Report2008.pdf).

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179-211.

Anderson, J. C., and Gerbing, D. W. 1988. "Structural equation modeling in practice: A review and recommended two-step approach," *Psychological Bulletin (*103:3), pp. 411-423.

Bassellier, G., Benbasat, I., and Reich, B.H. 2003. "The influence of business managers' IT competence on championing IT," *Information Systems Research* (14:4), pp. 317-336.

Bandura, A. 1986. Social foundations of thoughts and action: a social cognitive theory, Englewood Cliffs, NJ: Prentice Hall.

Baron, R. M., and Kenny, D. A. 1986. "The moderator-mediator variable distinction in social psychological research: Conceptual, strategic and statistical considerations," *Journal of Personality and Social Psychology* (51:6), pp. 1173-1182.

Bhattacherjee, A., and Premkumar, G. (2004). "Understanding Changes in Belief and Attitude toward Information Technology Usage: A Theoretical Model and Longitudinal Test," *MIS Quarterly,* (28:2), pp. 229-254.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., and Boss, R. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

Brown, S.A., and Venkatesh, V. 2005. "Model of adoption of technology in households: A baseline model test and extension incorporating household life cycle," *MIS Quarterly (*29:3), pp. 399-426.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, (34:3), pp. 523-A527.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004a. "A Model for Evaluating IT Security Investments," *Communications of the ACM* (47:7), pp. 87-92.

Chan, M., Woon I., and Kankanhalli A. 2005. "Perceptions of information security at the workplace: linking information security climate to compliant behavior," *Journal of Information Privacy and Security* (1:3), pp. 18-41.

Chin, W.W. 1998. "The partial least squares approach for structural equation modeling," *Modern Methods for Business Research,* G.A. Marcoulides (Hrsg.). Mahwah, New York: Lawrence erlbaum associates Publishers, pp. 295-336.

Crossler, R. E. and Bélanger, F. 2006. "The effect of computer self-efficacy on security training effectiveness," in *Proceedings of the 3rd annual conference on information security curriculum development,* ACM Press, New York, USA, pp. 124–129.

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

Diamantopoulos, A., and Winklhofer, H. M. 2001. "Index construction with formative indicators: An alternative to scale development," *Journal of Marketing Research (*38:2), pp. 269-277.

Dinev, T., and Hu, Q. 2007. "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems* (8:7), pp. 386-408.

Ernst and Young 2003. *Global Information Security Survey*, New York, http://www. Security management.com/archive/library/EY_Survey1103.pdf

Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research,* Reading: Addison-Wesley.

Fornell, C., and Larcker, D.F. 1981. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18:1), pp. 39-50.

Frank, J., Shamir, B., and Briggs, W. 1991. "Security-related behavior of pc users in organizations," *Information and Management* (21:3), pp. 127-135.

Fulk, J., Steinfield, J., and Power, G. 1987. "A scoial information processing model of media in organizations," *Communication Research* (14:5), pp. 529-552.

Furnell, S. M. 2006. "Remote pc security: Securing the home worker," *Network Security* (11), pp. 6-12.

Gaston, S. J. 1996. *Information security: Strategies for successful management,* Toronto: CICA Publishing.

Galvez, S. M., and Guzman, I. R. 2009. "Identifying Factors that Influence Corporate Information Security Behavior." *in Americas Conference on Information Systems (AMCIS),* Paper 765.

Gefen, D., and Straub, D. 2005. "A practical guide to factorial validity using PLS-graph: Tutorial and annotated example," *Communications of the AIS* (16:1), pp. 91-109.

Hair, J. F., Anderson, R. E., Tatham, R. L., and Black, W. C. 1998. *Multivariate data analysis*, Englewood Cliffs, NJ: Prentice Hall.

Herath, T., and Rao, H. R. 2009a. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems* (47:2), pp. 1-12.

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

Jarvis, C., Mackenzie, S., and Podsakoff, P. 2003. "A critical review of construct indicators and measurement model misspecification in marketing and consumer research," *Journal of Consumer Research (*30:2), pp. 199-218.

Leach, J. 2003. "Improving user security behavior," *Computers & Security (*22:8), pp. 685-693.

Lee, J. and Lee, Y. 2002. "A holistic model of computer abuse within organizations," *Information Management and Computer Security*, (10:2), pp. 57- 63.

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

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for common method variance in cross-sectional research designs," *Journal of Applied Psychology*, (86:1), pp. 114-121.

Loch, K. D., Straub, D. W., and Kamel, S. 2003. "Diffusing the internet in the Arab world: The role of social norms and techological culturation," *Engineering Management* (50:1), pp. 45–63.

Moore, G. C., and Benbasat, I. 1991. "Development of an instrument to measure the perceptions of adopting an information technology innovation," *Information Systems Research* (2:3), pp. 192-222.

Ng, B.Y., and Rahim, M.A. 2005. "A socio-behavioral study of home computer users' intention to practice security," in *Proceedings of the 9th Pacific Asia Conference on Information Systems*, Bangkok, Thailand.

NIST 2003. "Building an information technology security awareness and training program," M. Wilson (eds.), Gaithersburg: National Institute of Standards and Technology, NIST Special Publication, pp. 800-50, retrieved from http://csrc.nist.gov/publications/nistpubs/

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, pp. 156-166.

Petter S., Straub D., and Rai, A. 2007. "Specifying formative constructs in information systems research," *MIS Quarterly (*31:4), pp. 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology,* (88:5), pp. 879-903.

Rezgui, Y., and Marks, A. 2008. "Information security awareness in higher education: An exploratory study," *Computers & Security (*27:7-8), pp. 241–253.

Rhee, H.-S., Kim, C., and Ryu, Y.U. 2009. "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers & Security* (28:8), pp. 1-11.

Ringle, C.M., Wende, S., and Will, A. 2005. Smartpls. Hamburg, Germany: SmartPLS.

Rotvold, G. 2008. "How to create a security culture in your organization." *The Information Management Journal (*42:6), pp. 32-38.

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

Siponen, M., Mahmood, M. A., and Pahnila, S. 2009. "Are employees putting your company at risk by not following information security policies?" *Communications of the ACM* (52:12), pp. 145-147.

Siponen, M., and Vance, A. 2010. "Neutralization: New insight into the problem of employee information systems security policy violations," *MIS Quarterly* (34:3), pp. 487-502.

Sobel, M. 1982. "Asymptotic intervals for indirect effects in structural euquation models," *Sociological methodology*. Leinhart, S. (e.d.). San Francisco: Jossy-Bass, pp.290-312.

Spears, J. 2006. "The effects of user participation in identifying information security risk in business processes," in *Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research*, pp. 351-352.

Spears, J. L., and Barki, H. 2010. "User participation in information systems security risk management," *MIS Quarterly* (34:3), pp. 503-522.

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

Straub, D. W., and Welke, R.J. 1998. "Coping with systems risk: Security planning models for management decision making," *MIS Quarterly* (22:4), pp. 441-469.

Symantec. 2009. Symantec Internet Security Threat Report: Trends for 2008, Symantec Corporation, Cupertino, CA (available online at http://eval.symantec.com/mktginfo/enterprise/white_ papers/b-whitepaper_exec_summary_internet_security_threat_ report_xiv_04-2009.en-us.pdf).

Thomson, M. E., and von Solms, R. 1998. "Information security awareness: Educating your users effectively," *Information Management and Computer Security* (6:4), pp. 167-173.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2008. "Investigating information security awareness: Research and practice gaps," *Information Security Journal: A Global Perspective* (17:5-6), pp. 207-227.

Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. 2010. "Aligning security awareness with information systems security management," *Journal of Information System Security* (6:1), pp. 36-54.