Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Shaping intention to resist social engineering through transformational leadership, information security culture and awareness

Waldo Rocha Flores *, *Mathias Ekstedt*

Department of Industrial Information and Control Systems, Royal Institute of Technology (KTH), Stockholm, Sweden

ARTICLE INFO

Article history:
Received 19 November 2014
Received in revised form 13 January 2016
Accepted 16 January 2016
Available online 2 February 2016

Keywords:
Transformational leadership
Information security culture
Information security awareness
Theory of planned behavior
Social engineering
Mixed methods research

ABSTRACT

This paper empirically investigates how organizational and individual factors complement each other in shaping employees' intention to resist social engineering. The study followed a mixed methods research design, wherein qualitative data were collected to both establish the study's research model and develop a survey instrument that was distributed to 4296 organizational employees from a diverse set of organizations located in Sweden. The results showed that attitude toward resisting social engineering has the strongest direct association with intention to resist social engineering, while both self-efficacy and normative beliefs showed weak relationships with intention to resist social engineering. Furthermore, the results showed that transformational leadership was strongly associated with both perceived information security culture and information security awareness. Two mediation tests showed that attitude and normative beliefs partially mediate the effect of information security culture on employees' intention to resist social engineering. This suggests that both attitude and normative beliefs play important roles in governing the relationship between information security culture and intention to resist social engineering. A third mediation test revealed that information security culture fully explains the effect of transformational leadership on employees' attitude toward resisting social engineering. Discussion of the results and practical implications of the performed research are provided.

1. Introduction

Modern enterprises are heavily dependent of information systems. This dependency has led to enterprises being vulnerable to events that lead to those information systems being compromised. Consequently, managing risks to those systems are highly prioritized by firms worldwide. In fact, a survey conducted by Ernst and Young showed that 93% of companies globally are maintaining or increasing their investments in cyber-security to combat the ever increasing threat from cyber-attacks (Van Kessel and Allan, 2013). Traditionally, the predominant countermeasures have been of technical nature, and over the years the effectiveness and robustness of these measures have increased substantially. As a potential consequence, attackers have developed techniques to bypass these countermeasures by targeting employees accessing and using information systems in an organization (Applegate, 2009). It's a well-known fact that employees are the weakest link in an organization's defense against external information security

* *Corresponding author.* Tel.: +47 8 7906820.
E-mail address: waldorf@kth.se (W. Rocha Flores).
http://dx.doi.org/10.1016/j.cose.2016.01.004

threats. Attackers exploit this weakness by manipulating employees into performing actions that benefits the attacker, e.g., click on a malicious email links and install malware on their computers, or reveal personal computer passwords over telephone (Mitnick and Simon, 2002). These behavioral information security threats rely on psychological manipulation of people and goes under the name of social engineering.

The presence of new ways to compromise information security has moved the attention to the "human" element of information security management, that is, attitudes, beliefs, norms, behavioral patterns, leadership, culture, security awareness, etc. (Albrechtsen, 2007; Dhillon and Backhouse, 2001; Siponen, 2005), and how these factors influence information security behaviors. Several approaches focusing on the "human" side of information security management have been proposed. These approaches can roughly be divided in two categories: (1) approaches focusing on understanding why end-users *deliberately* comply or not comply with information security policies or how awareness of different countermeasures such as security training influences information system misuse (e.g., J. D'Arcy et al., 2008); (2) approaches focusing on understanding why social engineering is successful. The first category is the most dominant. Studies in this category offer theoretically grounded methods, and empirical evidence on the effectiveness of tested theories, including theory of planned behavior (Bulgurcu et al., 2010), neutralization theory (Siponen and Vance, 2010), learning theory (Warkentin et al., 2011), organizational narcissism (Cox, 2012), and protection motivation theory (Ifinedo, 2012). The literature related to the second category, which this paper pertains to, offers recommendations on "social" countermeasures such as security awareness training, the use of intranet sites dedicated to information security, communication of information classification policies, and communication of password polices (Applegate, 2009; Huang et al., 2009; Peltier, 2006). "Technical" countermeasures have also been proposed to prevent phishing (email-based social engineering), including filter and content analysis tools detecting phishing at the server-side, and blacklist-based approaches preventing users to access malicious websites (Huang et al., 2009). Other social engineering research has focused on success rates of unannounced phishing experiments (e.g., Hasle et al., 2005; Jagatic et al., 2007; Dodge et al., 2007; Bakhshi et al., 2009; Mohebzada et al., 2012), or providing empirical results on characteristics that explain an individual's social engineering susceptibility through simulated attacks (e.g., Dhamija et al., 2006; Karakasiliotis et al., 2006; Downs et al., 2007; Pattinson et al., 2012; Halevi et al., 2013).

However, a review of the social psychology, management, and security literature by Workman (2008) showed that no theoretical framework specifically related to social engineering security threats had been developed. Hence, there is a lack of social engineering studies providing theoretically grounded methods, and empirical evidence on their effectiveness (with an exception of Workman, 2007; Rocha Flores, Holm, Svensson, & Ericsson, 2014; Rocha Flores, Holm, Nohlberg, & Ekstedt, 2015a). Furthermore, the effect of key organizational constructs proposed in organizational and individual behavior literature on information security has not been rigorously examined (Hu et al., 2012). We argue that there is a need for more research studies to obtain a better understanding of how organizational and individual constructs complement each other in shaping information security behaviors.

Collecting data on actual security behaviors is challenging (Crossler et al., 2013). Many behavioral information security studies have therefore instead focused on capturing employees' intention to perform a given security behavior (e.g., intention to comply with information security policies) (e.g., Bulgurcu et al., 2010; Warkentin et al., 2011; Ifinedo, 2012). The reason researchers have focused on measuring intentions is that intention is, according to the theory of planned behavior, an immediate antecedent of actual behavior (Ajzen et al., 2004). As intention is used to predict actual behavior in many information security studies, it is important to investigate if intention predicts actual information security behavior. We have therefore conducted empirical studies where actual social engineering security behavior was measured using both written hypothetical scenarios wherein respondents were asked to envision their behaviors in actual social engineering attack scenarios (self-reported behavior) and by using phishing experiments (observed behavior). The empirical study included 2018 organizational employees, and identified a significant correlation between employees' intention to resist social engineering and actual social engineering security behavior. These results are published in Rocha Flores et al. (2015a, 2015b). Based on the empirical fact that intention can be used to understand actual social engineering security behaviors, we aim at obtaining an understanding of what shapes employees' intention to resist social engineering. This was supported by developing a theoretical model that investigates how organizational and individual factors complement each other in shaping employees' intention to resist social engineering. To attain this first aim of the study the following research question was formulated:

> *RQ1: Which organizational factors have a significant influence on employees' perceptions about social engineering security threats and, in turn, their intention to resist social engineering?*

The conceptual model of the research purposes of the study is presented in Fig. 1. The rest of the paper is structured as follows. In section 2, the theoretical background related to social engineering is presented together with a presentation of limitations in the existing literature. In section 3, the research model of the study is established through an exploratory study. The section that follows presents the confirmatory study testing the proposed research model in order to answer the study's

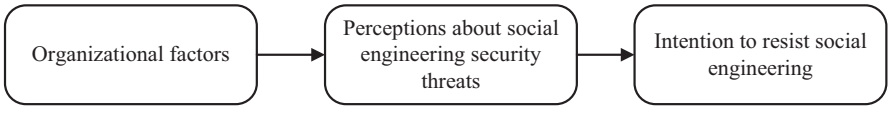

Fig. 1 – Conceptual model of the study.

research question. Finally, the paper ends with a discussion of the results and conclusions of the work.

2. Theoretical background and limitations in the existing literature

Social engineering is an external information security threat that includes exploiting human weaknesses by manipulating people into performing actions that benefit an attacker (Mitnick and Simon, 2002). Social engineering is today a major security threat to organizations, and is often launched through email (phishing) or phone (phone fraud). In order to combat social engineering it is important to understand why some employees resist social engineering attacks better than others. Previous theoretical literature has proposed reasons why individuals fall victim to social engineering. For instance, employees who exhibit a greater trust are more likely to be deceived. A perpetrator can use this to his or her advantage by impersonating an important user such as a senior manager or a member of the IT service team to gain a victim's trust (Laribee et al., 2006). Using insider lingo and name-dropping of "common colleagues" can also be used to gain a victim's trust and thereby make the victim comply with a "malicious" request (Nohlberg, 2009). Perpetrators can attempt to establish interpersonal relationships with victims to create a feeling of commitment. Attempting to make a victim react to exclusive offers is believed to make a victim comply with a "malicious" request as people are in general more eager to buy something that is exclusive and offered for a short time of period (Nohlberg, 2009) (Thornburgh, 2004) (Cialdini, 2006).

Existing empirical work on social engineering can be dived two categories: papers providing empirical results through simulated attacks and papers providing empirical results through unannounced phishing experiments. These works are discussed next.

Papers relying on simulated attacks present empirical results on how respondents would behave in the event of an attack by imitating a social engineering attack. A web-based role play exercise including 232 participants aimed at identifying significant predictors of phishing success (Downs et al., 2007). A deeper understanding of the web environment was found to be associated with being less vulnerable to phishing, while perceived severity of consequences of successful phishing did not predict phishing susceptibility. Dhamija et al. (2006) provides empirical evidence about which malicious strategies are successful in deceiving users. In a usability study, 22 participants were shown 20 web sites and asked to determine which ones were fraudulent. The results showed that 23% of the participants did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time. A web-based survey, which presented a mix of 20 legitimate and illegitimate emails to 179 participants, was used to assess social engineering susceptibility (Karakasiliotis et al., 2006). The survey asked participants to classify the emails and explain the rationale for their choices. The result showed that 36% of the participants successfully identified the legitimate emails, while 45% of the participants successfully spotted the illegitimate ones. In sum, although the use of simulated attacks provides empirical data that are valuable to understand why employees are vulnerable to social engineering, one critical limitation is that the studies do not provide accurate results on how individuals perform in actual attack scenarios. One remedy to this limitation is to conduct social engineering assessments wherein the participants are not aware that their security behavior is being measured. Logically, researchers have attempted to obtain a better sense of the actual level of security among individuals by conducting social engineering security assessments in the form of unannounced phishing experiments. However, most of the studies have been conducted in a university environment using students as the empirical sample. For instance, Jagatic et al. (2007) phished university students in order to acquire students' login information, and investigated if including context information related to the victim in the email increases the probability for a successful attack. The results showed that when context data gathered from social networks are used in the email, 72% of the students submitted valid logins, while when not using context data collected from social networks, 16% fell for the attack. West Point Military Academy used phishing experiments to train their students to more effectively manage phishing (Dodge et al., 2007). Their approach was to conduct two phishing attacks, and assess if training efforts given by discussing the first attack were effective. The first attack deceived 80% of the students, while the second only managed to deceive 40%. Mohebzada et al. (2012) conducted a phishing exercise in a university community and performed two phishing attacks that targeted 10000 university faculty, staff and students. The results showed that 8.7% fell for the first attack and 2% fell for the second attack. Finally, Halevi et al. (2013) conducted an empirical study among university students that investigated the role of different personal characteristics in explaining why people fall victim to social engineering. The study identified neuroticism as the strongest predictor.

This article aims at providing information about how organizational and individual factors complement each other in shaping organizational employees' intention to resist social engineering. Therefore, a limitation in the current literature is that the aforementioned unannounced phishing experiments have not been conducted using organizational employees as the empirical sample. The unannounced phishing experiments that have used organizational employees as the sample have drawn their conclusions based on success rates of conducted social engineering attacks, i.e., the percentage of employees that succumb to the attack. One, such study is based on an experiment conducted by Bakhshi et al. (2009), wherein a phishing mail was sent out to organizational employees as a means to provide empirical evidence of how many employees succumb to social engineering. The experiment was ceased after approximately 3.5 h. During that period of time, 23% of recipients were fooled by the attack. The email included factors related to how the attacker constructs the attack (e.g., trusted e-mail source, attention-grabbing subject, type of social engineering technique used) in order to understand why people fall victim to social engineering. A phishing audit was done by Hasle et al. (2005) wherein two tests against a subset of organizational employees were performed. The first test comprised a survey wherein the participants were asked to submit their login information in order to authenticate if they were to win a prize.

The second test comprised an e-mail which triggered a login box. In their tests approximately 30% of the targets submitted their passwords. While these two studies provide empirical evidence of how many organizational employees succumb to social engineering, they have one critical limitation: they fail in examining which organizational and individual factors shape social engineering security behavior. At present moment, only the studies by Workman (2007) and the authors of this paper (Rocha Flores et al., 2014, 2015a, 2015b) have conducted unannounced phishing experiments using organizational employees as the research sample and examined which factors explain employees' susceptibility to social engineering. Hence, there is need for more research studies addressing these questions. The present paper addresses these questions using intention to resist social engineering as the study's dependent variable. As our previous research has shown significant relationship between intention to resist social engineering and actual social engineering security behavior (Rocha Flores et al., 2015a) (Rocha Flores et al., 2015b), we argue that using intention to resist social engineering as the study's dependent variable is valid to understand which factors shape social engineering security behavior.

3. Research model development

This study followed a mixed method research design, and was carried out through two main stages: an exploratory stage and a confirmatory stage. These stages are depicted in Fig. 2. The first reason for employing an exploratory study was that knowledge of variables relevant to social engineering and security awareness was not fully obtained. The second reason was that relevant quantitative instruments were not available. The exploratory stage both resulted in the establishment of the study's research model and informed the second, quantitative stage wherein a measurement instrument was developed and used to empirically test the research model. This methodology is known as a mixed method research design (also labeled as multi-method research design and pluralist methodology) (Creswell and Plano Clark, 2011). Fig. 2 illustrates the research process which is based on the suggestions by previous work (Creswell and Plano Clark, 2011; Lee, 1991; MacKenzie et al., 2011; Trochim and Donnelly, 2006). This section describes the research and result of the exploratory stage. The confirmatory stage is described in section 4.

The aim of the first, exploratory stage was to identify study constructs and establish the research model. This aim was fulfilled by collecting qualitative data through six semi-structured interviews with a sample of content experts. The section that follows presents a description of how the data in the exploratory stage were collected.

3.1. *Exploratory data collection*

The six respondents included in the interviews were all experienced individuals working with information security on a regular basis for 5–20 years. Of the six respondents, three worked as senior information security consultants at two different information security consultancy firms; one worked as head of information security at a software application development firm, and the final two respondents were currently academics but with many years of practical experience as information security consultants, and they were chosen based on recommendations from peers. Four of the respondents were geographically located in Sweden, one in Finland (but working extensively in Sweden) and the last one in the USA. As the purpose of the exploratory stage was to gain an insight into factors shaping social engineering security behavior – in order to develop hypotheses for a more definite investigation – the number of respondents was deemed to be sufficient for this phase of the research. Furthermore, the sixth and last interview did not produce any new radical insights into the respondents' view of the phenomena. The literature recommends that interview data should be collected until theoretical saturation take place and a too high number of respondents will make thorough interpretations of the interviews difficult (Kvale, 1986). Three of the interviews were carried out face-to-face at the respondent's respective places of business, and three were carried out over telephone due to geographical concerns. The interviews lasted between 60 and 150 minutes and were audio-recorded and transcribed. Handwritten notes were also taken by the interviewer and transcribed electronically. The interviews all had the same general approach, and consisted of two main objectives: to gain a deeper understanding of important factors for shaping social engineering security behavior and to discuss potential relationships between factors. Before the interviews we obtained a general understanding of social engineering and factors that might have an effect on behaviors. This was obtained by surveying the literature. To obtain the respondents' opinions about important factors, open questions were asked but explicitly targeting factors related to social engineering security behavior. The original layout and scope of the interviews were somewhat changed according to the areas or factors that the respondents wanted to discuss. For

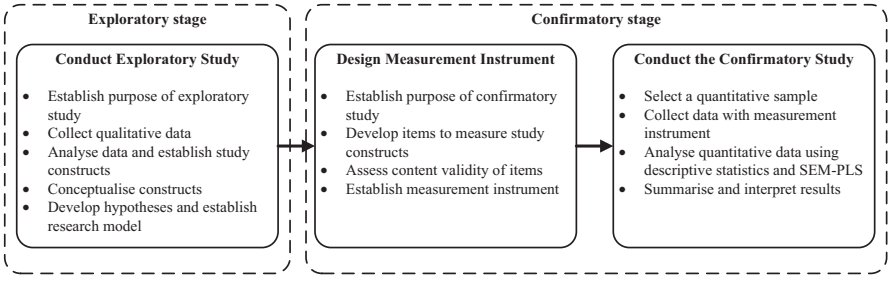

Fig. 2 – Main stages of the study.

example, no answers were forced, and the respondents were allowed to discuss a particular area in greater detail. As a consequence, more time was spent on those matters the respondents perceived to be of greater importance for the topic of the study.

The combination of surveying the literature and conducting interviews yielded a first pool of seven constructs, which then led us to conceptualize the constructs in order to avoid problems with construct validity (due to measurement issues) and statistical conclusion validity (due to biasing effect of measurement model misspecification) of the model (MacKenzie et al., 2011). An appropriate conceptualization of constructs is important for several reasons (Jarvis et al., 2003): first, a poor construct definition leads to confusion about what the construct does and does not refer to; and second, developed measurement items may not represent the focal construct or overlap with other constructs due to not being adequately defined.

The conceptualization of constructs had, in this study, three main objectives: 1) provide a clear, concise and unambiguous conceptual definition of the constructs; 2) specify the conceptual theme of the constructs (e.g., assessing if the construct is unidimensional or multidimensional); 3) evaluate the comprehensiveness of the constructs' dimensions (i.e., the relevance each dimension has to its focal construct and if any dimensions are missing to capture its construct). In line with those objectives, the two following steps were carried out: first, effort was spent on defining the constructs as clear and unambiguous as possible; second, a web survey – capturing data on our proposed conceptual definitions, our assessment of the constructs conceptual theme, and the comprehensiveness of the constructs' dimensions – was designed and distributed to 120 content experts. The respondents were identified from scientific articles from searches in professional societies' databases such as the IEEE and in pure indexing databases such as SCOPUS. When selecting people to serve as raters, it is important to make sure that they have sufficient intellectual ability to understand and complete the survey (Hinkin and Tracey, 1999). We therefore argue that the raters both need to have knowledge in the field of information security and have sufficient intellectual ability. Consequently we approached content domain experts to act as raters. Using content experts, rather than members from enterprises, has shown to provide reliable results and is commonly used in health research where the quality of measurement instrument is of significant importance (Lynn, 2006). Furthermore, MacKenzie et al. (2011) recommends using content experts in the early phase of the instrument development phase.

In all, 18 respondents completed the survey. The number of respondents is satisfying as, when assessing comprehensiveness of included variables, it is recommended to include a minimum of three experts, while using more than ten is probably unnecessary (Lynn, 2006). To capture data on our conceptual definitions and assessment of the construct conceptual theme, open-ended questions were included. To assess the dimensions' relevance, the respondents were questioned to give their opinion on the degree of association the experts believed each dimension has to its focal construct. For each dimension the respondents were asked to assess the degree of association each dimension has to its focal construct using a five-point Likert scale ranging from 1 to 5, where 1 = not associated, 2 = somewhat associated, 3 = quite associated, 4 = highly associated, and 5 = very highly associated. Inspired by Stalmeijer et al. (2008), it was decided to eliminate dimensions that rated below 3.5 but also considering experts' comments on why they believed the dimension was not relevant to its construct. Open-ended questions were included to assess both any important dimension missing to capture the construct domain, and the understandability of the dimensions, i.e., if the dimensions are named properly or should be renamed. For the interested reader, the complete results and changes to the instrument can be found in Rocha Flores and Korman (2012). The following subsection presents the main findings from the exploratory study which aimed to develop the study's research model.

3.2. *Results of the exploratory study*

First, and in line with the objective of the study, it was decided that social engineering security behavior was to be used as the endogenous study variable in the study. However, as we in our previous research identified significant correlation between intention to resist social engineering and actual social engineering security behavior (Rocha Flores et al., 2015a, 2015b), intention was later decided to function as the dependent variable for this particular research paper.

The exploratory stage of the study resulted in three classes of constructs: organizational structure, information security awareness, and intrinsic beliefs (also known as positive physiological traits) about an employees' social engineering security behavior. Constructs (i.e., the study's independent variables) and example of respondent statements supporting their inclusion are provided in Table 1 (no examples of respondent statements are provided for intrinsic beliefs as they were identified by surveying the literature previous to the interviews).

The conceptualization process included all study constructs, except the intrinsic belief constructs (self-efficacy, attitude, and normative beliefs) as these items were already proven reliable by previous empirical research (Bulgurcu et al., 2010; Cox, 2012; Ifinedo, 2012). The process resulted in the decision that one of the constructs was multidimensional – namely, information security awareness. Information security awareness was defined as a formative second-order construct composed of two reflective first-order constructs: general information security awareness and information security policy awareness. This construction is referred to as a type II second-order construct model (Jarvis et al., 2003). The other constructs were assessed to be unidimensional and operationalized as first-order constructs.

Comments from the experts indicated that one construct was less relevant. This construct (perceived learning oriented environment) is based on social learning theory (Bandura, 1977). After considering the comments and the argument to not include too many different theoretical concepts in a theoretical model including variables from the theory of planned behavior (Sommestad and Hallberg, 2013) led us to remove this construct. The final six constructs that were used to establish the study's research model are presented in Table 2 together with their conceptual definition.

Table 1 – Derived constructs from the interviews.

Class	Construct	Examples of respondent statements
Organizational structure	Transformational leadership (TL)	"All kinds of measures can be implemented and employees can be trained, but without strong leadership to educate personnel, measures will not be effective. Strong leadership gives effective operational measures."
	Information security culture (ISC)	"You can implement a thousand polices, but they will not be accepted if they don't fit to the cultural environment within the organization. Some policies might be more accepted by employees working in a certain environment, while others will find the policies irrelevant with regards to the type of environment they work in." "There are individuals in an organization that behave insecurely regardless of formal organizational directives. It is difficult to shape individual behavior, it is therefore important to shape an organization, and by doing so employees will be influenced by each other. For instance, by looking at how colleagues behave the behavior of a single employee can potentially be influenced".
Information security awareness	Information security awareness (ISA)	"Making employees aware of common information security threats is critical." "Training users to recognize and react to social engineering attacks provide good results."
Intrinsic beliefs	Self-efficacy (SE)	
	Attitude (A)	
	Normative beliefs (NB)	

3.3. *Hypotheses development*

Based on the exploratory study and our understanding of causal links between endogenous and exogenous variables, the hypotheses were formed, and a research model aiming at investigating the influence of organizational structure, information security awareness, and intrinsic beliefs on intention to resist social engineering. In the following, hypotheses are formally stated and arguments identified from literature supporting their relevance are presented.

3.3.1. *The role of intrinsic beliefs*

The constructs categorized as intrinsic beliefs, namely attitude, normative beliefs and self-efficacy, pertain to the theory of planned behavior, which is one of the most well established theories in the behavioral sciences (Sommestad and Hallberg, 2013), and an extension of the theory of reasoned action (Ajzen and Fishbein, 1980) (Fishbein and Ajzen, 1975). The complete theory composes five constructs: attitude, normative beliefs, perceived behavior control, and behavior (Ajzen, 1991). The central factor of the theory is the individual's intention to perform a behavior in question, and the general rule is that the stronger the intention toward the behavior, the more likely it is that the behavior is performed. Variances in intention are explained by an individual's attitude toward the behavior, subjective norms, and perceived behavior control. Although the original theoretical model includes perceived behavior control, Fishbein and Ajzen (2011) found that difference between the constructs perceived behavior control and self-efficacy belief was weak and non-significant, and in Ajzen (1991) the two constructs are used interchangeably (in the present paper we from hereinafter use self-efficacy belief rather than perceived behavioral control). According to the theory of planned behavior, self-efficacy belief positively moderates the effect of intentions on behavior. However, this moderation hypothesis has received only limited empirical support (Ajzen, 1991). Therefore, the present research paper does not include an investigation of self-efficacy's potential moderating effect between intention and actual behavior. This is left for future research. We limit our investigation to the analysis of the direct effect of attitude, normative beliefs, and self-efficacy on in-

Table 2 – Conceptual definition of constructs.

Construct	Conceptual definition
Transformational leadership (TL)	A leader's actions to generate awareness and motivate employees to change their information security behaviors.
Information security culture (ISC)	An employee's individual perception of shared beliefs and values among colleagues in the work environment.
Information security awareness (ISA)	An employee's individual perception of both his/her general knowledge about information security and his/her cognizance of the information security policy.
General information security awareness (GISA)	An employee's individual perception of his/her own awareness of general information security phenomena such as value of assets, threat exposure given circumstances, vulnerabilities and risks.
Information security policy awareness (ISPA)	An employee's individual perception of his/her own cognizance of the actual information security policies in the organization.
Self-efficacy (SE)	An employee's judgment of personal skills, knowledge, or competency about of resisting social engineering.
Attitude (A)	The degree to which the performance of the information security behavior is positively valued.
Normative beliefs (NB)	An employee's perceived social pressure about his/her social engineering security behavior caused by behavioral expectations of such important referents as executives, colleagues, and managers.
Intention (I)	An employee's intention to resist social engineering

tention to resist social engineering. Hence, the study's first three hypotheses are proposed as follows:

H1. An employee's self-efficacy about resisting social engineering positively influences intention to resist social engineering.

H2. An employee's attitude toward resisting social engineering positively influences intention to resist social engineering.

H3. An employee's normative beliefs about resisting social engineering positively influence intention to resist social engineering.

3.3.2. *The role of information security awareness*

The role of information security awareness was suggested to influence social engineering security behavior. As the examples of interview respondent statements in Table 1 show, the respondents perceived that it is critical for employees to be aware of information security threats and also able to recognize and react to common deceptive social engineering techniques used by attackers. Achieving employee information security awareness has been recognized as a critical outcome of information security management programs (Kayworth and Whitten, 2010; Werlinger et al., 2009). Therefore, studies within the domain of social engineering have focused on assessing information security awareness in order to identify strategies to increase the employees' awareness of common social engineering threats (Dodge et al., 2007; Karakasiliotis et al., 2006; Rocha Flores et al., 2014).

This paper defines information security awareness as an employee's general knowledge about information security threats, and his or her knowledge of specific information security policies related to social engineering threats. This means the following. An employee can be aware of threats related to information security based on past experience or interest. The employee can also have knowledge about specific policies, which might require him or her to undergo specific training on policies which makes him or her aware of how acceptable use of IT products and services is described in the organization's policy or how the policy governs management of sensitive and confidential information. Hence, information security awareness can be shaped by an employee's own interest and experiences or by interventions carried out by the organization's information security management group.

The theory of planned behavior argues that factors such as experience and knowledge can influence behavior indirectly by influencing behavioral, normative, and control beliefs, and this effect has been tested and identified to have a positive effect in the domain of information security policy compliance (Bulgurcu et al., 2010). This serves as the premise to propose the hypotheses related to information security awareness, self-efficacy and attitude:

H4a. An employee's information security awareness is positively associated with self-efficacy regarding resisting social engineering.

H4b. An employee's information security awareness is positively associated with attitude toward resisting social engineering.

3.3.3. *The role of information security culture*

The respondents interviewed in the explorative stage of the study perceived that an organizational culture shaping information security behavior should be taken into account. Organizational culture has been defined in many ways. In this study the definition by Schein (1984) was adopted by defining culture as "a pattern of basic assumptions that a group of individuals has developed in learning to cope with its problems of external adaptation and internal integration" (Schein, 1984). These assumptions are considered to be valid and therefore govern appropriate behavior in relation to those problems, in a group of individuals (Inkpen & Tsang 2005). Furthermore, organizational culture is related to employees' perception of shared beliefs and values among employees in the work environment, and points out the quality (e.g., richness and friendliness) of social relationships at the workplace (Chow and Chan, 2008). This implies that shared organizational culture should influence individuals' beliefs and therefore form a given behavior. In information security contexts, Chang and Lin (2007) found that organizational culture significantly influenced information security measures (confidentiality, availability, and accountability). Therefore, it is a logical deduction to believe that in the context of social engineering, this fostering environment that information security culture creates has a direct association with an employee's information security awareness, attitude and normative beliefs about information security threats. The following hypotheses are therefore proposed:

H5a. An organization's information security culture is positively associated with an employee's information security awareness.

H5b. An organization's information security culture in the organization is positively associated with an employee's attitude toward resisting social engineering.

H5c. Information security culture in the organization is positively associated with an employee's normative beliefs about resisting social engineering.

In a systematic review of quantitative studies that have empirically investigated variables influencing information security policy compliance by Sommestad et al. (2013), it revealed that security culture defined as "the overall environment fosters security-minded think" is a weak predictor of intention to comply with an organization's information security policies. This result indicates that other factors could be more important for behavioral intention in security contexts, or that other factors underlie and explain the relationship between information security culture and behavioral intention. We, therefore, intend to study the relationship between information security culture and behavioral intention in more depth by hypothesizing that the relationship between information security culture and intention to resist social engineering is mediated by attitude and normative beliefs. Hence:

H5d. The relationship between information security culture and intention to resist social engineering is mediated by an employee's attitude toward resisting social engineering.

H5e. The relationship between information security culture and intention to resist social engineering is mediated by an employee's normative beliefs about resisting social engineering.

3.3.4. *The role of transformational leadership*

The behavior of security executives was suggested to influence employees' social engineering security behavior. As the examples of interview respondent statements in Table 1 show, the respondents perceived that strong and motivating leadership makes user security training efforts more effective.

A vast amount of studies have explored the link between leadership behaviors and organizational outcomes (e.g., perceived employee job satisfaction and leader effectiveness), but the results have been inconsistent (see reviews by Boal and Hooijberg, 2000; Carpenter et al., 2004). Although the research studies agree that executive leadership is important for organizational outcomes, there is still a lack in understanding *how* executives influence organizational performance (Wang et al., 2011). A leadership style that has been associated to the adoption of a certain behavior is transformational leadership. According to Bass and Riggio (2006) and Dvir et al. (2002), transformational leadership emphasizes follower perceptions, cognitions, and emotional responses to the leaders of an organization. Transformational leadership occurs when leaders expand and elevate subordinate interests so that they focus on the good of the organization, generate awareness and acceptance of the group's purpose, and motivate employees to look beyond their own self-interest for the good of the group. In the context of information security, the concept points out that the leader should articulate a security vision so that all employees can easily and clearly understand the objectives of information security efforts in the organization. The leader should also show a reasonable level of mastery, and make it clear for each employee what role he or she plays in the organization's information security efforts, what his or her responsibility is and whom to turn to in case of a security concern. The information security leader's actions should portray information security efforts as business-supportive, collective and should promote understanding and cooperation as means to achieve and maintain effective information security. Finally, the information security leader's actions should set expectations, as well as provide contingent reward (i.e., punishing non-compliance and negligence while rewarding success stories and exemplary behavior). The following hypothesis is suggested:

H6a. Transformational leadership has a positive direct effect on the information security culture in the organization.

H6b. Transformational leadership has a positive direct effect on an employee's information security awareness.

Although studies have shown that leadership behavior has a direct effect on intrinsic beliefs, there is evidence that the relationship between leadership behavior and individual beliefs might be a result of the effect of organizational culture. For instance, both the functionalist and the attribution perspective in the organizational culture literature argue that leadership influences culture directly (Tsui et al., 2006). Organizational culture, as previously mentioned, then directly influences beliefs and behaviors in a given group. Therefore, obtaining a deeper understanding of the relationship between leadership behavior and individual beliefs is necessary – and could identify if organizational culture has a significant role in governing the relationship between transformational leadership and belief outcomes. As such, the study aims at investigating both the direct and indirect effect of transformational leadership on employees' attitude toward preventing social engineering by conducting a mediation analysis. Hence:

H6c. The relationship between transformational leadership and an employee's attitude toward resisting social engineering is mediated by the organization's information security culture.

3.3.5. *Control variables*

Control variables are considered to be variables that are not explicitly linked to the hypotheses in the research model and theories that the model is built on. Oftentimes control variables are included automatically or blindly without arguing why these are included and why these are assumed to produce distortions in the observed relationships (Spector and Brannick, 2010). In this study, two control variables are included – namely, age of the respondent, and computer experience. The control variables are, in the research model, directed to the study's dependent variable, that is, they control for variance in intention to resist social engineering. The two control variables are included as their influence on social engineering behavior has previously been tested by other researchers. Age has been studied on previous occasions with disparate results (Dhamija et al., 2006; Sheng et al., 2010; Workman, 2008). While Sheng et al. (2010) identified that those younger were more susceptible to phishing than other age groups, Workman (2008) found that older individuals were more susceptible to phishing, and Dhamija et al. (2006) did not identify a significant relationship between age and the degree of susceptibility to phishing. Computer experience has been studied on several occasions and operationalized in various ways, e.g., as general knowledge of computer and as the number of hours an individual spends on a computer each week (Moos and Azevedo, 2009; Rhee et al. 2009). This study controls for computer experience by operationalizing computer experience as the number of years an employee has utilized information technology products and services (e.g. computers, Internet access, electronic mail, etc.).

To conclude the section in which the description of how the research model was developed, the complete model, with the hypotheses included, is presented in Fig. 3.

4. Confirmatory study

4.1. *Item development*

The first step in the confirmatory study was to generate a set of measurement items that represent the conceptual domain

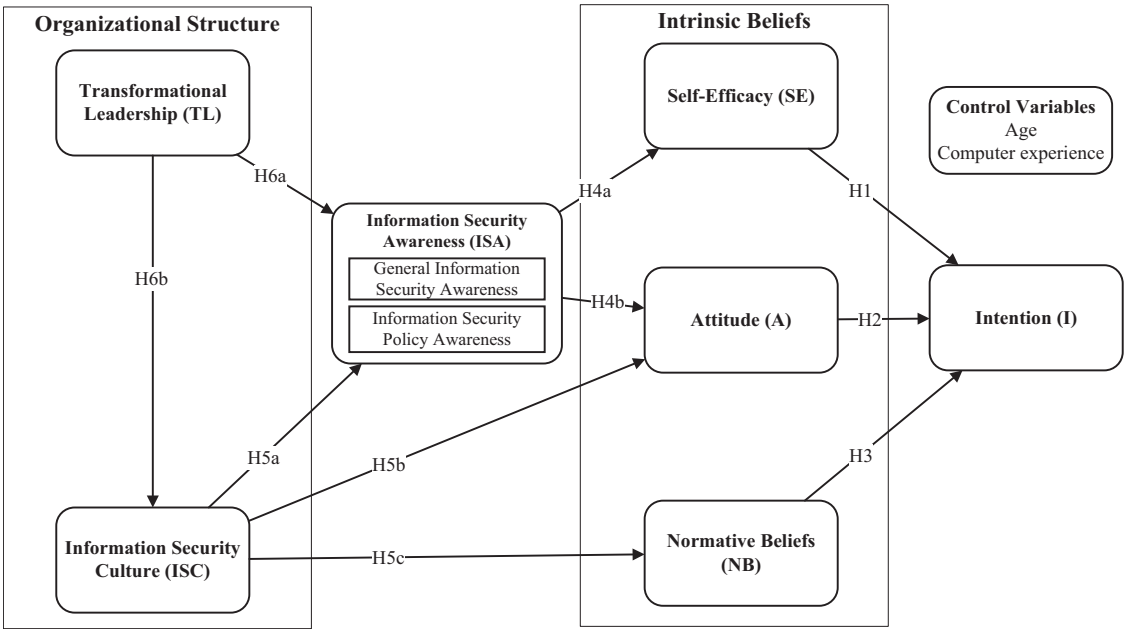

Fig. 3 – Proposed research model. Notes: The mediation hypotheses H5d, H5e, and H6c are not depicted in the figure.

of each study construct. Measurement items can be identified through: conducting reviews of the literature; deduction from the theoretical definition of the construct; previous theoretical and empirical research on the focal construct; suggestions from experts in the field; and an examination of other items of the construct that already exist (Nunnally and Bernstein, 1994). In order to assure that the measurement instrument includes items that actually capture the theoretical meanings of each construct (i.e., establish construct validity) in the research model, effort was placed on the instrument validation process, as recommended by MacKenzie et al. (2011). In our study, we first spent effort on deciding how the items were related their focal construct, i.e. if they were to be specified as reflective or formative items. The distinction between those two types of items is critically important as Monte Carlo simulations reported by Jarvis et al. (2003) and Petter et al. (2007) suggest that structural parameter estimates can be biased when indicators that should be modeled as having formative relationships with a construct are modeled as having reflective relationships. Thus, in the process of selecting items and develop scales, the nature of the relationship between the indicators and the construct they are intended to represent should be considered. All first-order constructs were specified with multiple reflective items (as previously mentioned information security awareness was defined as a formative second-order construct composed of two reflective first-order constructs). All items were inspired on existing scales, but adapted and rewritten for the context of our study. Hence, all items were developed specifically for this study. Items representing intrinsic belief constructs and intention were identified from previous work (e.g., Bulgurcu et al., 2010; Ifinedo, 2012; Cox, 2012). We attempted to develop the intrinsic belief and intention items in the context of social engineering security attacks. Therefore, the items were written in a form that conveys information about social engineering. For instance, for the intention construct, we included phrases such as: "… I suspect that the request originates from a non-legitimate sender …", "… who I suspect of being non-legitimate from installing malicious software …", "… who I suspect of being unauthorized or non-legitimate from gaining access to my work computer by means of a security attack." Items representing general information security awareness were based on Bulgurcu et al. (2010) and adapted to this study; items representing information security policy awareness were based on the interviews with the experts, wherein specific policies related to social engineering threats were discussed (Rocha Flores and Antonsen, 2013): in the development of items capturing information security culture the studies by Knapp et al. (2007) and Chow and Chan (2008) worked as inspiration and the items were then adapted to our study, and items to measure transformational leadership were based on existing scales (Bass and Riggio, 2006; Dvir et al., 2002) and adapted to the context of this study.

4.2. *Content validity assessment*

When developing new items, MacKenzie et al. (2011) recommends to assess the content validity of the items before colleting primary data. Content validity, "the degree to which items in an instrument reflect the content universe to which the instrument will be generalized (Straub et al., 2004, p. 424)", is an assessment that consists of two stages: development and judgment-quantification (Lynn, 2006). The development stage consists of identification of study constructs, item generation, and instrument. Judgment-quantification entails asking a number of experts to evaluate the validity of the items and as a set (DeVellis, 1991). In the present study, we quantitatively assessed the content validity using the item-sorting method proposed by Anderson and Gerbing (1991). This was done for all constructs except intrinsic belief constructs and intention as these items were already proven reliable by

previous empirical research. Besides providing a statistical result to assess the adequacy of content validity of each item, the method does not make any implicit assumptions about the direction of the relationship between the items and their corresponding factors or about the correlations between the items themselves. Therefore, it can be used to assess the content validity of either formative or reflective indicators. This is a fundamental advantage when developing formative items to capture a construct as a lack of content validity is a particularly serious problem for constructs with formative indicators (Petter et al., 2007). The investigated items were tested for their content validity by collecting data using an email survey distributed to 452 content domain experts, of which 51 completed the survey. We also asked for comments on wording, if the survey items were clearly understood and if they perceived that any items were missing to represent the constructs. Based on this pre-test the measurement instrument was revised, and the initial item pool containing 46 developed items was reduced to 32 items with an adequate degree of content validity (for more information on specific changes, the interested reader is referred to Rocha Flores and Antonsen, 2013). The results lead to all constructs was specified with multiple items.

4.3. *Pilot test*

The final survey was directed to IT users from a variety of organizations and industries. To ensure that the survey was adapted to this sample, we wanted to pilot test the survey before employing it in the primary data collection phase. The result from the content validity study yielded 32 items capturing 4 constructs, and by adding 17 items representing intention, self-efficacy, attitude, and normative beliefs the survey included 49 items. We perceived that the number of items were too many for a survey. Therefore, we revised the survey and kept those items with the highest degree of content validity, which yielded a survey with 1–7 items per construct, and 36 items in total, all measured on a 11-point licker scale from 0 to 10 inspired by Paternoster and Simpson (1996) and Siponen and Vance (2010).

The pilot survey was developed in Swedish, and distributed to 200 employees known to the researchers and working in different organizations and industries. After one reminder 47 employees had completed the survey. The survey asked for comments on wording, if the survey items were clearly understood and if the survey could be improved. Based on this pre-test minor corrections were made to the wording of the items. Then, the instrument was proofread by a professional translation and interpreting company. The final survey that was used to collect and analyze data is outlined in Appendix A.

4.4. *Primary data collection*

The survey was sent out to 4296 employees from organizations operating in a variety of industries. Data was collected between January 2013 and October 2013. The data collection procedure was identical for each of the participant organizations. The survey was hosted by a widely used internet-based application (SurveyMonkey). As compensation to the participant organizations, they were offered a presentation of their results benchmarked against other organizations overall and within their industry. Two reminders were sent to non-responding participants after a first week and a third week in order to increase the response rate. After two reminders 1583 respondents had completed the survey, which gives an effective response rate of 37%. The respondents in the sample represent organizations from a diverse set of industries. Demographic characteristics of respondents are presented in Table 3.

Table 3 – Demographic characteristics of respondents.

Gender	Male	1037	66%
	Female	546	34%
Age (years)	18–24	15	1%
	25–34	254	16%
	35–44	452	29%
	45–54	485	31%
	55 or older	377	24%
Computer experience (years)	1–4	9	1%
	5–9	22	1%
	10–14	165	10%
	15–20	499	32%
	20 or more	888	56%
Industry	Education	2	0%
	Government	7	0%
	IT/Entertainment	39	2%
	Financial services	14	1%
	Healthcare	15	1%
	Energy	1092	69%
	Transportation	2	0%
	Water and Wastewater	16	1%
	Manufacturing	333	21%
	Retail/Wholesale	12	1%
	Municipality	32	2%
	Telecommunication	3	0%
	Other	16	1%
Company size	Less than 100	107	7%
	100–499	31	2%
	500–999	117	7%
	1000–5000	1260	80%
	More than 5000	68	4%

4.5. *Data analysis techniques*

Partial least squares structural equation modeling (PLS-SEM) was used to test the measurement model's psychometric properties and structural model. The variance-based technique, PLS-SEM, was used instead of covariance-based techniques due to three reasons. First, PLS-SEM does not require large samples. The study by Reinartz et al. (2009) showed that variance-based techniques offer better estimation than other techniques in samples under 250. The sample size of the current study is 1583; however, the multigroup analysis employed for examining the moderating effect of national culture included a sample of 100 each per country. Second, the study's model includes a second order formative construct (ISA) in the model, and PLS-SEM is better suited for better handling potential indeterminacy problems than other techniques such as LISREL (Joreskog and van Thillo, 1972). Third, PLS-SEM is a non-parametric technique; hence, there is no need to guarantee the normality of the data (Hair et al., 2011).

Before assessing the quality of the measurement model, the data set was first screened, using SPSS (version 19) (IBM Corporation, 2010), to identify any outliers as recommended by Hair et al. (2011). This process yielded the identification of four outliers, which were removed for further analysis. The software package SmartPLS (version 2.0.M3) (Ringle et al., 2005) was then used for the estimations. To interpret and analyze the structural model, a two-step approach to structural modeling was used (Barclay et al., 1995): first, the quality of the measurement model was assessed to ensure the validity and reliability of the items; second, the structural model was analyzed in order to test the hypotheses and quality of the structural model, further described in section 4.6 and 4.7 below.

4.6. *Quality of measurement model*

The reflective measures were assessed through internal consistency reliability, indicator reliability, and convergent validity and discriminant validity. Cronbach's alpha (CA) and composite reliability (CR) should be higher than 0.7 for adequate internal consistency reliability (Hair et al., 2011). As the second and third column in Table 4 shows, all values are above the threshold (>0.7). This suggests adequate internal consistency reliability. Indicator loadings should be higher than 0.7 for acceptable indicator reliability (Hair et al., 2011). As Table 5 shows, all indicators load to their respective construct with a value above or close to (ISC 3 = 0.688) the threshold value (>0.7). This suggests that problems with indicator reliability were not an issue in this study. If the average variance extracted (AVE) yields a value above 0.5, convergent validity is established. Looking at Table 4, we can see that all values are above the threshold; we can therefore conclude that convergent validity was ensured. Discriminant validity is established if the two following requirements are fulfilled: the square root of each constructs' AVE is higher than the correlation with any other construct, and indicator loadings are higher than all of its cross loadings (Hair et al., 2011). As Table 4 shows, the square root value of each constructs' AVE (diagonal values in bold) is higher than all values on the rows below. Table 5 shows that indicator loadings (values in bold) are higher than all of its cross loadings (values to the right of indicator loadings). Those two premises lead to the conclusion that the criterion for discriminant validity is satisfied. In conclusions, all validation tests suggest that the items are both valid and reliable and could thus be used to evaluate the structural model.

4.7. *Evaluation of structural model*

In order to assess the significance of the structural path coefficients, bootstrapping re-sampling with 1583 cases and 5000 re-samples was used. Critical t-values for a two-tailed test are 1.65 (significance level = 10%), 1.96 (significance level = 5%), and 2.58 (significance level = 1%) (Hair et al., 2011). The R^2 values of the endogenous constructs measure how much variance is explained by the exogenous constructs. R^2 values of 0.67, 0.33, or 0.19 can be described as substantial, moderate, or weak, respectively (Chin, 1988). As Fig. 4 shows, all hypotheses proposing direct effect between constructs in the research model could be accepted (the testing of hypotheses H5d, H5e, and H6c proposing mediating effects is described in section 4.8).

The R^2 value for the dependent variable intention is 0.42, which indicates that the constructs in the model explain 42% of the variance in the dependent variable. Thus, the proposed model explains a moderate amount of variance in intention. Information security awareness explains 24% of the variance in self-efficacy; information security awareness together with information security culture explains 18% of variance in attitude; information security culture explains 21% of variance in normative beliefs and together with transformational leadership explains 41% of variance in information security awareness. Finally, transformational leadership explains 27% of variance in information security culture. As information security awareness was operationalized as formative second-order construct, the significance of the first-order weights was examined. The weights indicated that each dimension significantly contributes to their underlying construct. Among the constructs from the theory of planned behavior, attitude has the strongest direct effect on intention, with a regression coefficient of $\beta = 0.57$. The impact of self-efficacy and normative beliefs on intention is significant but weak, with $\beta = 0.09$ and $\beta = 0.08$, respectively. The association between information security awareness and self-efficacy is significant, with $\beta = 0.50$. The association between information security awareness is weaker, but still significant, with $\beta = 0.27$. The direct effect of information security culture on information security awareness, attitude, and normative is significant with $\beta = 0.17$, $\beta = 0.24$, and $\beta = 0.46$ respectively. Finally, transformational leadership has significant direct effect on both information security culture on information security awareness, with $\beta = 0.52$ and 0.53 respectively.

Table 4 – Correlations, Cronbach's alpha (CA), composite reliability (CR) and average variance extracted (AVE).

	CA	CR	AVE	A	GISA	I	TL	ISPA	NB	SE	ISC
A	0.925	0.947	0.817	**0.904**							
GISA	0.830	0.922	0.855	0.390	**0.624**						
I	0.883	0.914	0.681	0.637	0.330	**0.575**					
TL	0.944	0.957	0.816	0.218	0.509	0.367	**0.606**				
ISPA	0.880	0.918	0.736	0.323	0.561	0.264	0.407	**0.638**			
NB	0.952	0.965	0.873	0.421	0.324	0.343	0.395	0.346	**0.498**		
SE	0.918	0.942	0.803	0.371	0.469	0.330	0.386	0.446	0.349	**0.590**	
ISC	0.887	0.911	0.594	0.349	0.412	0.256	0.527	0.412	0.417	0.355	0.596

Values in bold highlight the criterion values that the values beneath shall be lower than.

Table 5 – Indicator loadings and cross loadings for reflective indicators.

	A	I	GISA	ISL	ISPA	NB	SE	ISC
A1	**0.901**	0.572	0.364	0.214	0.308	0.374	0.335	0.307
A2	**0.922**	0.633	0.364	0.228	0.304	0.389	0.331	0.336
A3	**0.896**	0.533	0.360	0.199	0.295	0.381	0.343	0.334
A4	**0.896**	0.560	0.320	0.143	0.258	0.377	0.333	0.281
I1	0.600	**0.839**	0.317	0.167	0.270	0.289	0.308	0.249
I2	0.574	**0.876**	0.303	0.168	0.237	0.337	0.290	0.250
I3	0.503	**0.838**	0.253	0.115	0.193	0.250	0.244	0.183
I4	0.449	**0.777**	0.235	0.105	0.168	0.232	0.214	0.171
I5	0.479	**0.793**	0.242	0.123	0.205	0.298	0.295	0.186
GISA1	0.329	0.284	**0.926**	0.488	0.621	0.282	0.411	0.394
GISA2	0.392	0.327	**0.923**	0.453	0.600	0.318	0.457	0.368
TL1	0.203	0.158	0.475	**0.891**	0.600	0.384	0.348	0.481
TL2	0.243	0.188	0.476	**0.880**	0.557	0.350	0.360	0.445
TL3	0.187	0.144	0.474	**0.906**	0.557	0.371	0.352	0.482
TL4	0.174	0.131	0.436	**0.932**	0.526	0.342	0.347	0.479
TL5	0.177	0.132	0.433	**0.907**	0.499	0.331	0.335	0.491
ISPA1	0.264	0.217	0.545	0.519	**0.882**	0.294	0.361	0.374
ISPA2	0.259	0.220	0.534	0.500	**0.877**	0.267	0.389	0.296
ISPA3	0.243	0.196	0.559	0.569	**0.845**	0.305	0.392	0.388
ISPA4	0.342	0.271	0.629	0.497	**0.828**	0.321	0.389	0.357
NB1	0.421	0.344	0.325	0.388	0.352	**0.929**	0.300	0.434
NB2	0.401	0.353	0.318	0.396	0.344	**0.940**	0.315	0.444
NB3	0.364	0.269	0.285	0.348	0.296	**0.930**	0.343	0.420
NB4	0.384	0.309	0.281	0.338	0.295	**0.939**	0.349	0.408
SE1	0.344	0.306	0.440	0.369	0.426	0.331	**0.897**	0.320
SE2	0.294	0.292	0.409	0.369	0.412	0.284	**0.894**	0.326
SE3	0.320	0.278	0.413	0.328	0.375	0.306	**0.905**	0.325
SE4	0.372	0.307	0.419	0.315	0.385	0.328	**0.890**	0.303
ISC1	0.182	0.155	0.249	0.345	0.251	0.299	0.208	**0.760**
ISC2	0.214	0.155	0.225	0.257	0.219	0.233	0.199	**0.703**
ISC3	0.330	0.246	0.312	0.274	0.288	0.283	0.243	**0.688**
ISC4	0.238	0.167	0.283	0.364	0.285	0.346	0.241	**0.801**
ISC5	0.225	0.154	0.370	0.613	0.409	0.404	0.307	**0.807**
ISC6	0.299	0.215	0.368	0.464	0.362	0.408	0.342	**0.842**
ISC7	0.386	0.286	0.370	0.409	0.349	0.431	0.331	**0.784**

Values in bold highlight the criterion values that the values beneath shall be lower than.

4.8. *Mediation analysis*

To test for mediation effect (H5d, H5e, and H6c) proposing mediating effects we followed the method suggested by Baron and Kenny (1986). Three tests for mediation were conducted independently: attitude mediates the relationship between information security culture and intention to resist social engineering; normative beliefs mediate the relationship between information security culture and intention to resist social engineering; and information security cultures mediate the relationship between transformational leadership and information security awareness. Table 6 shows the results from the mediation analysis and also supports a description of how the method was used in two steps. First, the significance of regression coefficients of each path independently of the mediating variable (MV) was assessed using bootstrapping resampling. That is, the mediating variable has not yet been introduced in the mediation model. Column 1 shows the results of this step. An initial requirement for investigating mediation effect is that all regression coefficients in column 1 should be significant (Baron and Kenny, 1986). As column 1 for the three tests shows, the regression coefficients for all paths are significant and thus fulfill the initial requirement. Second, the mediating variable is introduced to the model (shown in column 2). If path c is reduced, the mediating variable has an effect on the dependent variable (DV). If path c both reduces and becomes insignificant, the mediator fully mediates the effect of the independent variable (IV), and if path c reduces, but is still significant, the mediator partially mediates the effect between the IV and DV.

The mediation tests revealed that attitude partly mediates the effect of information security culture on intention to resist social engineering; normative beliefs partly mediate the effect of information security culture on intention to resist social engineering. Finally, the analysis revealed that information security culture partly mediates the effect of transformational leadership on information security awareness. Furthermore, as Table 7 shows, the coefficient of determination R^2 has higher value when the mediator variable is included in the path model.

To conclude this section, a summarization of the results of the hypotheses tests is presented in Table 8. An important note is that the hypotheses related to the testing for mediating effect (H5d, H5e, H6c) are presented in a different way than the rest of the hypotheses, because these hypotheses were investigated when conducting the analysis of mediation effect (cf. Table 6).

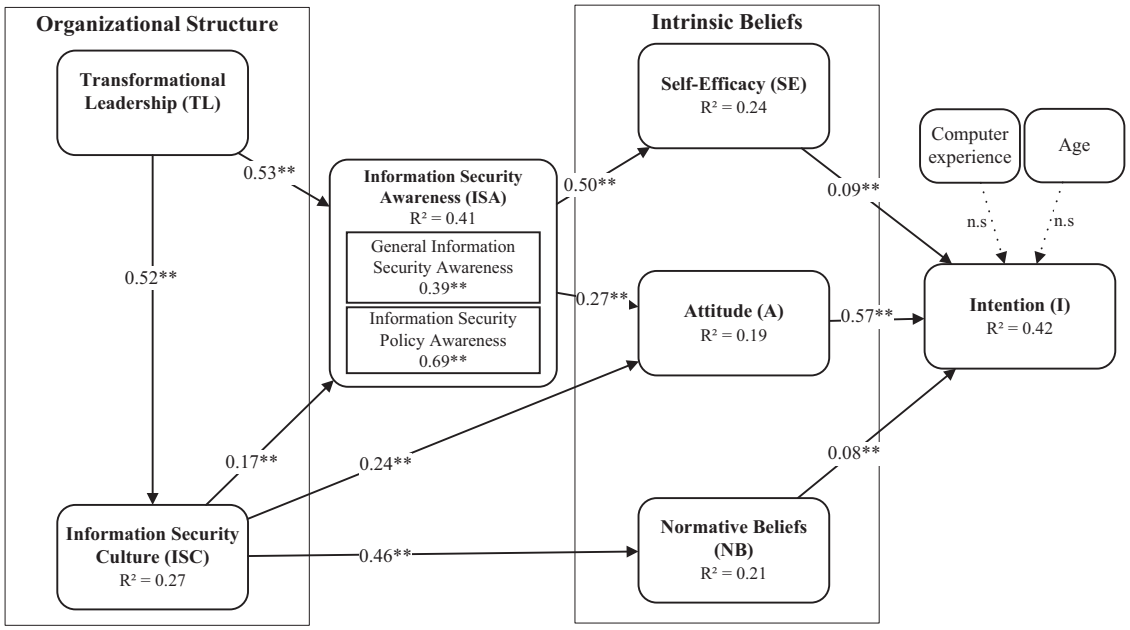

Fig. 4 – Results of structural model testing (full sample, n = 1583). Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at p < 0.05 and ** at p < 0.01.

4.9. *Addressing nonresponse bias and common method bias*

The data were collected via self-reported survey; thus, the potential for both nonresponse bias and common method bias (CMB) should be addressed (Podsakoff, 1986; Doty & Glick, 1998). To address potential nonresponse bias the last respondent method was used as recommended by Armstrong and Overton (1977) and previously used by researchers (Bulgurcu et al., 2010). The method assumes that non-respondents are like the projected last respondent in the last wave of data collection (final reminder). Inspired by the technique used in Bulgurcu et al. (2010) the dataset was split in three groups and a series of independent t-tests was conducted to identify any significant differences in means between the first and the last third of the respondents' data. If no significant differences between the first and the last third of the respondents' data on any of the measures analyzed are identified, nonresponse bias is not an issue in this study. This test procedure revealed no significant differences between the first and the last third of the respondents' data on any of the items analyzed. This suggests that nonresponse bias was not an issue in this study.

The threat of common methods bias (CMB) was addressed as follows. Ex ante, CMB was addressed by counterbalancing the order of questions in the questionnaire to discourage participants from figuring out the relationship between the dependent and independent variables that was attempted to be established. Further, the respondent's anonymity and providing no incentive for completing the survey reduced the likelihood of bias caused by social desirability or respondent acquiescence (Podsakoff et al., 2003). Ex-post, we performed a test for CMB recommended by Bagozzi et al. (1991) and used by Pavlou et al. (2007) wherein the correlation matrix was examined to identify any highly correlated constructs (r > 0.9). In our model, all constructs had correlations below the threshold (cf. Table 4). The ex-ante and ex-post tests suggest that the possibility of CMB is not of great concern and therefore it is unlikely that CMB confounds the interpretation of the results.

Table 6 – Mediation analysis results (full sample, n = 1583). The first column displays correlation before including the mediator variable, and the second column shows correlation with the mediator variable included.

IV:ISC			IV:ISC			IV:ISLB		
MV:A			MV:NB			MV:ISC		
	1	2		1	2		1	2
Path a (ISC→A)	0.354**	0.354***	Path a (ISC→NB)	0.458**	0.458**	Path a (ISLB→ISC)	0.522**	0.522**
Path b (A→I)	0.635**	0.620***	Path b (NB→I)	0.339**	0.277**	Path b (ISC→A)	0.354**	0.332**
Path c (ISC→I)	0.263**	0.044*	Path c (ISC→I)	0.263**	0.136**	Path c (ISLB→A)	0.215**	0.042*n.s*
	Partial mediation			Partial mediation			Full mediation	

Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at p < 0.05 and ** at p < 0.01.

Table 7 – R^2 values for paths without and without the mediator variable included.

Path	R^2
ISC→I:	0.069
ISC→A→I	0.405
ISC→I:	0.069
ISC→NB→I	0.130
ISLB→A:	0.046
ISLB→ISC→A	0.126

Notes: The conceptual definition can be found in Table 2.

5. Discussion and conclusions

5.1. *Significant organizational and individual information security factors*

This paper has empirically examined how factors on organizational and individual level influence an individual's intent to defend against social engineering. A research model was developed and empirically tested with data from 1583 Swedish employees. The empirical tests of the model showed that attitude has the strongest direct relationship with intention to resist social engineering (β = 0.57), while both self-efficacy (β = 0.09) and normative beliefs (β = 0.08) showed weak relationships with intention to resist social engineering. Results from research in information security policy compliance contexts including self-efficacy and normative beliefs have found stronger direct relationships between these two variables and intention to comply with information security policies. The systematic review by Sommestad et al. (2013) showed that that weighted mean of regression coefficients for attitude were 0.38; for subjective norm 0.20; and self-efficacy 0.20. The results from our study show that attitude toward resisting social engineering is the strongest predictor. This could be explained by the fact that social engineering resilience is based on an employee's way of thinking about social engineering. Holding an attitude that it is important and necessary to adapt to a resilient behavior and believing that adapting this behavior will have a positive outcome seem to be more important for behavioral intention than perceived ability or pressure from peers.

The results showed that the direct effect of information security culture on behavioral intention is weak. This result is in line with the results from studies in other information security contexts. For instance, Dugo (2007) found that the direct effect of security culture on intention to comply with information security policies is weak. Our mediation analysis revealed that attitude and normative beliefs underlie and explain the relationship between information security culture and behavioral intention. Of these two mediating variables, attitude showed to have a stronger role in explaining the effect of information security culture on intention to resist social engineering. When the attitude construct was included in the mediation model, the relationship between information security culture and intention to resist social engineering was still significant but decreased to almost zero. This implies that information security culture by itself has little or no direct effect

Table 8 – Results of the testing of hypotheses in the study.

Path	Supported/ rejected	Path coefficient	*p*-value
H1: An employee's self-efficacy about resisting social engineering positively influences intention to resist social engineering.	Supported	0.09	**
H2: An employee's attitude toward resisting social engineering positively influences intention to resist social engineering.	Supported	0.57	**
H3: An employee's normative beliefs about resisting social engineering positively influence intention to resist social engineering.	Supported	0.08	**
H4a: An employee's information security awareness is positively associated with self-efficacy regarding resisting social engineering.	Supported	0.50	**
H4b: An employee's information security awareness is positively associated with attitude toward resisting social engineering.	Supported	0.27	**
H5a: An organization's information security culture is positively associated with an employee's information security awareness.	Supported	0.17	**
H5b: An organization's information security culture in the organization is positively associated with an employee's attitude toward resisting social engineering.	Supported	0.24	**
H5c: Information security culture in the organization is positively associated with an employee's normative beliefs about resisting social engineering.	Supported	0.46	**
H5d: The relationship between information security culture and intention to resist social engineering is mediated by an employee's attitude toward resisting social engineering.	Supported	N/A	N/A
H5e: The relationship between information security culture and intention to resist social engineering is mediated by an employee's normative beliefs about resisting social engineering.	Supported	N/A	N/A
H6a: Transformational leadership has a positive direct effect on the information security culture in the organization.	Supported	0.53	**
H6b: Transformational leadership has a positive direct effect on an employee's information security awareness.	Supported	0.52	**
H6c: The relationship between transformational leadership and an employee's attitude toward resisting social engineering is mediated by the organization's information security culture.	Supported	N/A	N/A

Notes: n.s indicates statistically nonsignificant; * indicates statistical significance at $p < 0.05$ and ** indicates. Statistical significance at $p < 0.01$.

and that attitude plays a significant role in governing the relationship between information security culture and an employee's intention to resist social engineering.

Our third mediation analysis tested if organizational culture had a significant role as a mediator of the relationship between transformational leadership and employees' attitude toward resisting social engineering threats. The results showed that information security culture indeed has a significant role in shaping employees' attitude by fully mediating the effect of transformational leadership on employees' attitude toward resisting social engineering. Hence, information security culture fully explains the relationship between transformational leadership and employees' attitude in a social engineering context. In an information security policy context, a study by Hu et al. (2012) found no direct effect between perceived top management participation and attitude toward compliance with information security policies. The explanation provided by Hu et al. (2012) was the relative hierarchical distance between the top management and employees. This is certainly true, and our study disentangles the interrelated influences of leadership actions and organizational culture on attitude by showing that information security culture is the variable that realizes the effect of transformational leadership. Hence, transformational leadership lays the foundation to shape a culture promoting information security behaviors, which in turn directly influences employees' attitudes toward information security threats.

The model's constructs explain 42% of variance ($R^2 = 0.42$) in intention to resist social engineering, indicating that the model has a moderate explanatory power. Although attitude is predicted by two constructs (information security awareness and information security culture) and has the strongest direct effect on intention resist social engineering, the explanatory power is weak ($R^2 = 0.19$). The explanatory power is, however, stronger in our study than in the study conducted by Hu et al. (2012), which was conduected in the context of information security policy compliance ($R^2 = 0.14$). The results are similar for self-efficacy and normative beliefs; however, these constructs are predicted by one construct each (information security awareness and information security culture, respectively). This implies that other or more constructs should be included for a better prediction model if one of the intrinsic belief constructs is used as the dependent variable. As attitude toward information security threats indeed has a strong effect on intention to resist social engineering, which in turn has a significant correlation to actual social engineering security behavior, there is a need to complement the existing research by obtaining a deeper understanding of what are the factors that shape employees' attitude toward security threats. The direct and indirect effects of transformational leadership and direct effect of information security culture explain 41% of variance ($R^2 = 0.41$) in an employee's information security awareness, which indicates that these two constructs have a moderate explanatory power and important for explaining variances in an employee's information security awareness.

We have presented limitations in the extant research in the behavioral information security field. Further, our review of the literature in social engineering research shows a significant gap of empirical studies aiming at understanding how to shape employees' intention to resist social engineering. This study, therefore, complements the existing research by offering theoretical explanation and empirical evidence on what drives an employee to resist information security attacks. To the best of our knowledge, this is the first study that investigates this particular issue.

In summary, employees' attitude toward resisting social engineering has the strongest direct association with intention to resist social engineering, while both self-efficacy and normative beliefs showed weak relationships with intention to resist social engineering. An organization's information security culture has a significant direct effect on both attitude and normative beliefs about resisting social engineering, where information security culture has stronger effect on normative beliefs. Furthermore, attitude and normative beliefs play important roles in governing the relationship between information security culture and intention to resist social engineering. Transformational leadership is strongly directly associated with both perceived information security culture and information security awareness. Transformational leadership has no direct association with employees' attitude toward resisting social engineering. The reason is that information security culture fully explains this relationship. This answers the first research question posed by the study (RQ1).

5.2. *Managerial implications, limitations and future work*

Firms worldwide invest a vast amount of money to ensure information security throughout their organization. Although those investments are highly prioritized, knowing how to shape employees' behavioral intentions related to managing information security threats is still challenging. The results from our empirical investigation can support managers in their decision-making process by offering insights into social engineering threats in practice. Our results show that it is important for organizations to change their employees' beliefs about information security threats. Employees both need to be made aware of the benefits with protecting their computers systems (or risk by not doing so) and different manipulative techniques that social engineers use to trick them into conducting malicious acts. However, just being aware of threats is not enough. People can be aware of things that are not good for them, but that does not mean that they will change their behaviors. If that would be the case there would be fewer smokers today. As our study shows employees' attitude toward preventing attacks need to be changed. Employees need to obtain an understanding of the importance and benefits of changing their information security behaviors. If they do not understand the reasons there is a risk that changes in behaviors will not occur. Therefore, organizations need to set expectations that employees should understand security risks both in theory and in practice (behavioral expectations). Furthermore, employees need to understand that learning about information security will lead to positive outcomes for them as individuals and for the organization as a whole. Personalizing and making the communicated information in security training programs tangible make the training personally relevant and understandable. By doing so, employees will more easily grasp the communicated information and also see the

outcomes of their security training. Combining this with practical exercises where employees learn how to actually prevent social engineering will more likely lead to a change in their security behaviors.

There exist several limitations which should be taken into account when interpreting the results. First, although our study identified that attitude toward resisting social engineering strongly predicts behavioral intention, the factors that explain variances of attitudes have a weak explanatory power. Hence, future research should either include other or more variables that could potentially be stronger determinants of attitudes toward resisting social engineering. Second, we did not test if characteristics of a firm (e.g. size, industry in which the firm operate in) yield differences in the research model. Differences between firms could be identified based on firm characteristics. We acknowledge the potential impact of these factors and therefore recommend including them in future work. Third, although our previous published research has shown that intention to resist social engineering significantly correlates with actual social engineering security behavior, it does not mean that changing attitudes is enough. Attitude and intentions are important predictors of security behaviors and increase employees' motivation to learn how to manage security threats in practice. However, research has shown that there are other factors that also could explain resilience to social engineering. For instance, employees who exhibit a greater trust has shown to be easier to deceive, hence are less resilient to social engineering (Rocha Flores et al., 2014; Workman, 2007). Employees that are more likely to take risks and not think about the consequences of their actions have shown to be more likely to fall victim to social engineering (Rocha Flores et al., 2014). Finally, an individual's inability to handle stress together with a lack of confidence (neuroticism) has shown to influence his/her resilience to security threats (Halevi et al., 2013). Could it be that employees that manage stress better in security contexts take the time to think twice when they are attacked also manage security threats better? Hence, should future security training programs include stress management? These factors have not been included in the theoretical model that was empirically tested in this paper. In order to obtain a deeper understanding of which factor explains both intention and actual social engineering security behaviors, these factors, among others, should be included in future developed research models.

Appendix A. Items for constructs

Transformational leadership

TL1: The Information Security Leader clearly expresses the aim of initiatives to improve information security within my organization.

TL2: The Information Security Leader in my organization demonstrates a reasonable level of knowledge of, and proficiency in, information security.

TL3: The Information Security Leader in my organization describes information security as a collective effort.

TL4: The Information Security Leader promotes common understanding, communication and cooperation as a means to achieve and maintain effective information security throughout my organization.

TL5: The Information Security Leader describes information security as a function that supports our business and our information assets.

Information security culture

ISC1: My colleagues would warn me if they saw me taking risks (e.g. insecure use of e-mail, downloading malicious software, or risky password practices).

ISC2: There is a strong team spirit in my department.

ISC3: I have a good relationship with my colleagues and other members of my organization.

ISC4: My colleagues expect me to warn them if I see them taking risks (e.g. insecure use of e-mail, downloading malicious software, or risky password practices).

ISC5: My organization takes the view that information security is a collective responsibility.

ISC6: My colleagues and I have the same ambitions and visions in terms of protecting our information assets from individuals who try to gain unauthorized access to these.

ISC7: My colleagues and I agree that it is important to protect our information assets from becoming infected with malicious software.

Information security awareness

ISA1: I am aware of how acceptable use of IT products and services (e.g. computers, the Internet, e-mail, etc.) is described in our policy.

ISA2: I am aware of how acceptable installation of software is described in our policy.

ISA3: I know how our policy governs management of sensitive and confidential information.

ISA4: I am aware of the potential threats and negative consequences that inadequate information security in my work can cause.

ISA5: I am aware of my obligations under our policy regarding the use and management of passwords for my work computer.

ISA6: I understand the risks posed by inadequate information security in general.

Attitude[1]

A1: I have a positive attitude to prevent unauthorized individuals from accessing confidential information, such as my work computer password.

A2: I have a positive attitude to prevent individuals from installing malicious software on my work computer.

A3: I have a positive attitude to identify unauthorized, unexpected or suspicious requests in e-mails.

[1] In the survey the wording "positive attitude" was defined as to or how highly respondents value adopting a behavior to defend against social engineering. A "positive attitude" was also described as something in the survey statements that is personally *important*, *necessary* and *advantageous*.

A4: I have a positive attitude to identify unauthorized, unexpected or suspicious requests to do with my work computer password.

NB1: Important individuals around me think that I will prevent unauthorized individuals from accessing confidential information, such as my work computer password.

NB2: Important individuals around me think that I will prevent individuals from installing malicious software on my work computer.

NB3: Important individuals around me think that I will identify unauthorized, unexpected or suspicious requests in e-mails.

NB4: Important individuals around me think that I will identify unauthorized, unexpected or suspicious requests to do with my work computer password.

SE1: I am confident about my ability to prevent unauthorized individuals from accessing confidential information, such as my work computer password.

SE2: I am confident about my ability to prevent individuals from installing malicious software on my work computer.

SE3: I am confident about my ability to identify unauthorized, unexpected or suspicious requests in e-mails.

SE4: I am confident about my ability to identify unauthorized, unexpected or suspicious requests to do with my work computer password.

I1: I will not install software if I suspect that the request originates from a non-legitimate sender.

I2: I intend to prevent anyone who I suspect of being non-legitimate from installing malicious software on my computer by means of a security attack.

I3: I will not disclose my computer password to anyone who I suspect is not a legitimate party or authorized to receive such information.

I4: I intend not to disclose my computer password to anyone who I suspect is not a legitimate party or authorized to receive such information.

I5: I will prevent anyone who I suspect of being unauthorized or non-legitimate from gaining access to my work computer by means of a security attack.

REFERENCES

Ajzen I. The theory of planned behavior. Organ Behav Hum Decis Process 1991;50(2):179–211.

Ajzen I, Fishbein M. Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall; 1980.

Ajzen I, Brown T, Carvajal F. Explaining the discrepancy between intentions and actions: the case of hypothetical bias in contingent valuation. Pers Soc Psychol Bull 2004;30(9):1108–21.

Albrechtsen E. A qualitative study of users' view on information security. Comput Secur 2007;26(4):276–89.

Anderson JC, Gerbing DW. Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. J Appl Psychol 1991;76(5):732–40.

Applegate SD. Social engineering: hacking the wetware! Inf Secur J A Glob Perspect Taylor & Francis 2009;18(1):40–6.

Armstrong JS, Overton TS. Estimating nonresponse bias in mail surveys. J Mark Res 1977;14:396–402.

Bagozzi RP, Yi Y, Phillips LW. Assessing construct validity in organizational research. Adm Sci Q 1991;36(3):421–58.

Bakhshi T, Papadaki M, Furnell S. Social engineering: assessing vulnerabilities in practice. Inf Manag Comput Secur 2009;17(1):53–63.

Bandura A. Social learning theory. Englewood Cliffs, NJ: Prentice Hall.; 1977.

Barclay D, Higgins C, Thompson R. The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration. Technol Stud 1995;2(2):285–309.

Baron RM, Kenny DA. The moderator-mediator variable distinction in social psychological research – conceptual, strategic, and statistical considerations. J Pers Soc Psychol 1986;51(6):1173–82.

Bass BM, Riggio RE. Transformational leadership. 2nd ed. Mahwah, NJ: Lawrence Erlbaum Associates; 2006.

Boal KB, Hooijberg R. Strategic leadership research. Leadersh Q 2000;11(4):515–49.

Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 2010;34(3):523–48.

Carpenter MA, Geletkanycz MA, Sanders WG. Upper echelons research revisited: antecedents, elements, and consequences of top management team composition. J Manage 2004;30(6):749–78.

Chang SE, Lin C-S. Exploring organizational culture for information security management. Ind Manag Data Syst Emerald Group Publishing Limited 2007;107(3):438–58.

Chin WW. The partial least squares approach to structural equation modeling. In: Marcoulides GA, editor. Mod methods bus res. Mahwah, NJ: Lawrence Erlbaum Associates.; 1988. p. 295–358.

Chow WS, Chan LS. Social network, social trust and shared goals in organizational knowledge sharing. Inf Manag 2008;45(7):458–65.

Cialdini RB. Influence: The psychology of persuasion. revised ed. Harper Business; 2006.

Cox J. Information systems user security: a structured model of the knowing–doing gap. Comput Human Behav 2012;28(5):1849–58.

Creswell JW, Plano Clark VL. Designing and conducting mixed methods research. 2nd ed. Thousand Oaks, CA: SAGE; 2011.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. Comput Secur 2013;32(1):90–101.

D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf Syst Res 2008;20(1):79–98.

DeVellis RF. Scale development: theory and applications. Newbury Park, CA: Sage; 1991.

Dhamija R, Tygar JD, Hearst M. Why phishing works. Proc SIGCHI Conf Hum Factors Comput Syst. ACM; 2006. p. 581–90.

Dhillon G, Backhouse J. Current directions in IS security research: towards socio-organizational perspectives. Inf Syst J 2001;11(2):127–53.

Dodge R, Carver C, Ferguson A. Phishing for user security awareness. Comput Secur 2007;26(1):73–80.

Doty DH, Glick WH. Common methods bias: does common methods variance really bias results? Organ Res Methods 1998;1(4):374–406.

Downs JS, Holbrook M, Cranor LF. Behavioral response to phishing risk. Proc anti-phishing Work groups 2nd Annu eCrime Res summit. ACM; 2007. p. 37–44.

Dugo TM. The insider threat to organizational information security: a structural model and empirical test. Auburn University; 2007.

Dvir T, Eden D, Avolio BJ, Shamir B. Impact of transformational leadership on follower development and performance: a field experiment. Acad Manag J 2002;45:735–44.
Fishbein M, Ajzen I. Belief, attitude, intention, and behavior: an introduction to theory and research. Reading, MA: Addison-Wesley; 1975.
Fishbein M, Ajzen I. Predicting and changing behavior: the reasoned action approach. New York: Taylor & Francis; 2011.
Hair J, Ringle C, Sarstedt M. PLS-SEM: indeed a silver bullet. J Mark Theory Pract 2011;19(2):139–52.
Halevi T, Lewis J, Memon N. A pilot study of cyber security and privacy related behavior and personality traits. Proc 22nd Int Conf World Wide Web companion. International World Wide Web Conferences Steering Committee; 2013. p. 737–44.
Hasle H, Kristiansen Y, Kintel K, Snekkenes E. Measuring resistance to social engineering. Inf Secur Pract Exp. Springer; 2005;132–43.
Hinkin TR, Tracey JB. An analysis of variance approach to content validation. Organ Res Methods 1999;2(2):175–86.
Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decis Sci 2012;43(4):615–60.
Huang H, Tan J, Liu L. Countermeasure Techniques for Deceptive Phishing Attack. 2009 Int Conf New Trends Inf Serv Sci. 2009. p. 636–41.
IBM Corporation. SPSS Statistics. IBM Corporation; 2010.
Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput Secur 2012;31(1):83–95.
Inkpen AC, Tsang EWK. Social capital, networks, and knowledge transfer. Acad Manag Rev 2005;30(2):146–65.
Jagatic TN, Johnson NA, Jakobsson M, Menczer F. Social phishing. Commun ACM ACM 2007;50(10):94–100.
Jarvis CB, MacKenzie SB, Podsakoff PM. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. J Consum Res The University of Chicago Press 2003;30(2):199–218.
Joreskog KG, van Thillo M. LISREL: A General Computer Program for Estimating a Linear Structural Equation System Involving Multiple Indicators of Unmeasured Variables. 1972 Nov 30.
Karakasiliotis A, Furnell S, Papadaki M. Assessing end-user awareness of social engineering and phishing. Aust Inf Warf Secur Conf. Citeseer; 2006. p. 60.
Kayworth T, Whitten D. Effective information security requires a balance of social and technology factors. MIS Quartely Exec 2010;9(3):303–15.
Knapp KJ, Marshall TE, Rainer RK, Ford FN. Information security effectiveness: conceptualization and validation of a theory. Eyob E, editor, Int J Inf Secur Priv IGI Global 2007;1(2):37–60.
Kvale S. Interviews. An introduction to qualitative research interviewing. Thousand Oaks, CA: Sage Publications; 1986.
Laribee L, Barnes DS, Rowe NC, Martell CH. Analysis and defensive tools for social-engineering attacks on computer systems. Inf Assur Work 2006;388–9. IEEE.
Lee AS. Integrating positivist and interpretive approaches to organizational research. Organ Sci 1991;2(4):342–65.
Lynn MR. Determination and quantification of content validity. Nurs Res 2006;35(6):382–6.
MacKenzie SB, Podsakoff PM, Podsakoff NP. Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques. MIS Q 2011;35(2):293–334.
Mitnick K, Simon W. The art of deception: controlling the human element of security. Control. Hum. Elem. Secur. Indianapolis Indiana: Wiley Publishing; 2002.
Mohebzada JG, El Zarka A, Bhojani AH, Darwish A. Phishing in a university community: Two large scale phishing experiments. 2012 Int Conf Innov Inf Technol. IEEE; 2012. p. 249–54.
Moos DC, Azevedo R. Learning with computer-based learning environments: a literature review of computer self-efficacy. Rev Educ Res 2009;79(2):576–600.
Nohlberg M. Why humans are the weakest link. Soc Hum Elem Inf Secur Emerg Trends Countermeas IGI Global; 2009. p. 15–26.
Nunnally JC, Bernstein I. Psychometric theory. 3rd ed. New York: McGraw Hill.; 1994.
Paternoster R, Simpson S. Sanction threats and appeals to morality: testing a rational choice model of corporate crime. Law Soc Rev 1996;30(3):549–84.
Pattinson MR, Jerram C, Parsons K, McCormac A, Butavicius M. Why do some people manage phishing emails better than others? Inf Manag Comput Secur Emerald Group Publishing Limited 2012;20(1):18–28.
Pavlou PA, Liang H, Xue Y. Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. MIS Q 2007;31(1):105–36.
Peltier TR. Social engineering: concepts and solutions. Inf Syst Secur Taylor & Francis Ltd 2006;15(5):13–21.
Petter S, Straub D, Rai A. Specifying formative constructs in information systems research. MIS Q 2007;31(4):623–56.
Podsakoff PM. Self-reports in organizational research: problems and prospects. J Manage 1986;12(4):531–44.
Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J Appl Psychol 2003;88(5):879–903.
Reinartz W, Haenlein M, Henseler J. An empirical comparison of the efficacy of covariance-based and variance-based SEM. Int J Res Mark 2009;26(4):332–44.
Rhee H-S, Kim C, Ryu YU. Self-efficacy in information security: its influence on end users' information security practice behavior. Comput Secur 2009;28(8):816–26.
Ringle CM, Wende S, Will A. SmartPLS. Hamburg: University of Hamburg; 2005.
Rocha Flores W, Antonsen E. The development of an instrument for assessing information security in organizations: Examining the content validity using quantitative methods. Proc 2013 Int Conf Inf Resour Manag. Natal, Brazil, May 22–24; 2013.
Rocha Flores W, Korman M. Conceptualization of Constructs for Shaping Information Security Behavior: Towards a Measurement Instrument. Proc th 7th Annu Work Inf Secur Priv. Orlando, Florida, USA, December 16; 2012.
Rocha Flores W, Holm H, Svensson G, Ericsson G. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Inf Manag Comput Secur 2014;22(4):393–406.
Rocha Flores W, Holm H, Nohlberg M, Ekstedt M. Investigating personal determinants of phishing and the effect of national culture. Inf Manag Comput Secur 2015a;23(2):178–99.
Rocha Flores W, Holm H, Nohlberg M, Ekstedt M. Investigating the correlation between intention and action in the context of social engineering in two different national cultures. In: The Hawaii International Conference on System Sciences (HICSS 48). Kauai, Hawaii: 2015b. p. 3508–17.
Schein EH. Coming to a new awareness of organizational culture. Sloan Manage Rev 1984;25(2):3–16.
Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J. Who falls for phish? Proc 28th Int Conf Hum factors Comput Syst – CHI '10. New York, New York, USA: ACM Press; 2010. p. 373.
Siponen M. An analysis of the traditional IS security approaches: implications for research and practice. Eur J Inf Syst 2005;14(3):303–15.

Siponen M, Vance A. Neutralization: new insights into the problem of employee systems security policy violations. MIS Q 2010;34(3):487–502.
Sommestad T, Hallberg J. A review of the theory of planned behaviour in the context of information security policy compliance. In: Janczewski LJ, Wolfe HB, Shenoi S, editors. Secur Priv Prot Inf Process Syst. Berlin, Heidelberg: Springer Berlin Heidelberg; 2013. p. 257–71.
Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf Manag Comput Secur Emerald Group Publishing Limited 2013;22(1):42–75.
Spector PE, Brannick MT. Methodological urban legends: the misuse of statistical control variables. Organ Res Methods 2010;14(2):287–305.
Stalmeijer RE, Dolmans DHJM, Wolfhagen IHAP, Muijtjens AMM, Scherpbier AJJA. The development of an instrument for evaluating clinical teachers: involving stakeholders to determine content validity. Med Teach [Internet]. Informa UK Ltd UK 2008;30(8):272–7.
Straub D, Boudreau M-C, Gefen D. Validation guidelines for IS positivist research. Commun Assoc Inf Syst 2004;13(1):380–427.
Thornburgh T. Social engineering: the dark art. Proc 1st Annu Conf Inf Secur Curric Dev. ACM; 2004. p. 133–5.
Trochim WMK, Donnelly JP. The research methods knowledge base. 3rd ed. Atomic Dog; 2006.
Tsui AS, Zhang Z-X, Wang H, Xin KR, Wu JB. Unpacking the relationship between CEO leadership behavior and organizational culture. Leadersh Q [Internet] 2006;17(2):113–37.
Van Kessel P, Allan K. Under cyber attack: EY's Global Information Security Survey 2013 [Internet]. 2013. Available from: http://www.ey.com/US/en/Newsroom/News-releases/News_Cyber-crime-is-greatest-global-threat-to-organizations-survival-today.
Wang H, Tsui AS, Xin KR. CEO leadership behaviors, organizational performance, and employees' attitudes. Leadersh Q [Internet] 2011;22(1):92–105.
Warkentin M, Johnston AC, Shropshire J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur J Inf Syst Nature Publishing Group 2011;20(3):267–84.
Werlinger R, Hawkey K, Beznosov K. An integrated view of human, organizational, and technological challenges of IT security management. Inf Manag Comput Secur Emerald Group Publishing Limited 2009;17((1):4–19.
Workman M. Gaining access with social engineering: an empirical study of the threat. Inf Syst Secur 2007;16(6):315–31.
Workman M. Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. J Am Soc Inf Sci Technol 2008;59(4):662–74.

Waldo Rocha Flores is a PhD student at the department of Industrial Information and Control Systems at the Royal Institute of Technology (KTH) in Stockholm, Sweden. He received his MSc degree in Electrical Engineering at the Royal Institute of Technology (KTH) in 2008, and his MSc degree in Business Administration and Economics at Stockholm university school of business in 2013. He does research in the field of information security governance and socio-organizational aspects of information security.

Mathias Ekstedt is Associate Professor at the Royal Institute of Technology (KTH) in Stockholm, Sweden. His research interests include systems and enterprise architecture modeling and analyses with respect to information and cyber security, in particular for the domain of electric power systems.