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

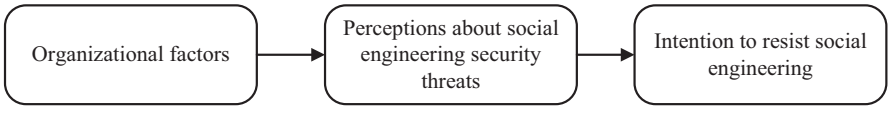

Fig. 1 – Conceptual model of the study.