


Chapter 18

Workplace Violence and Social Engineering Among Korean Employees

Youngkeun Choi

 <https://orcid.org/0000-0002-8842-9826>

Sangmyung University, Seoul, South Korea

ABSTRACT

The purpose of this study is to investigate if workplace violence has a negative influence on employees who are exposed to social engineering. This article explores if information security culture can be helpful to make them to resist social engineering. In the results, first, job-related bullying and abusive supervision decreases employees' intention to resist social engineering. Second, information security culture decreases the negative effect of job-related bullying, abusive supervision or organizational politics on employees' intention to resist social engineering.

1. INTRODUCTION

Recently, some of researches on information security have paid the attention to the “human” element of information security management, that is, attitudes, beliefs, norms, behavioral patterns, leadership, culture, security awareness, etc. (Glaspie & Karwowski, 2017; Sebescen & Vitak, 2017; Stewart & Jürjens, 2017), and how these factors influence information security behaviors. Several approaches focusing on the “human” side of information security management have been proposed. Some researchers have focused on understanding why end users deliberately comply or not comply with information security policies or how awareness of different counter measures such as security training influences information system misuse (D’Arcy et al., 2008; Bauer & Bernroider, 2017). Other researchers have been interested in why social engineering is successful. They offer 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 policies (Applegate, 2009; Peltier,

DOI: 10.4018/978-1-6684-7464-8.ch018

2006). Especially, they have focused on success rates of unannounced phishing experiments (Jagatic et al., 2007; Dodge et al., 2007; Bakhshi et al., 2009), or showed empirical results on characteristics that explain an individual's social engineering susceptibility through simulated attacks (Pattinson et al., 2012; Halevi et al., 2013).

However, Workman (2008) argued that no theoretical framework specifically related to social engineering security threats had been developed in the perspective of social psychology, management, and security literature. Hence, there is a lack of social engineering studies providing theoretically grounded methods, and empirical evidence on their effectiveness. 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).

Therefore, this study argues 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. For this, the purpose of this study is understanding what shapes employees' intention to resist social engineering. In order to combat social engineering, it is important to understand why some employees are more vulnerable to social engineering attacks than others. Generally, the employees who have complaints in organizations may be vulnerable to the attack of social engineering. Therefore, this study investigates what kinds of work environment have a negative influence on employees who are exposed to social engineering. And it explores what is the organizational factor to make them to resist social engineering.

2. THEORETICAL BACKGROUND AND HYPOTHESES DEVELOPMENT

Social engineering means an external information security threat that includes exploiting human weaknesses by manipulating people into performing actions that benefit an attacker (Junger et al., 2017; Mitnick & Simon, 2002). Recently, it is a major security threat to organizations, and is often launched through email (phishing) or phone (phone fraud) (Fan et al., 2017). 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 (Cialdini, 2006).

In order to better understand employees' intention to resist social engineering, the social bond theory can be applied. Hirschi (1969) presented attachment, commitment, involvement and belief are the four main factors in order to describe how individuals bond with social institutions and argued that men are intrinsically prone to deviance. Especially, the social bond theory describes how individuals, who have stronger social ties, engage less in deviant behavior. Deviance occurs when the social bond is weak or broken. The more an individual is bonded to an organization, the less likely he or she is to deviate from the organization's policies (Chapple et al., 2005). Most of studies have also applied the social bond theory to explain the delinquency of adolescents. Recently, social bond theory has been applied to adult criminality and organizational deviances.

People are the main issue in the human aspects of information security due to their direct contact with information. Their responsibility and commitment to safeguard information assets play a vital role in this domain (AlHogail, 2015). Commitment refers to the aspiration of acquiring a high-status job. Personal achievement and reputation are important to committed individuals (Cheng et al., 2013). They spend

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/workplace-violence-and-social-engineering-among-korean-employees/311273

Related Content

First Attempts to Formalize Some Main Aspects of Psychoanalysis: Towards a Computational Psychoanalysis

(2018). *Computational Psychoanalysis and Formal Bi-Logic Frameworks* (pp. 136-205).

www.irma-international.org/chapter/first-attempts-to-formalize-some-main-aspects-of-psychoanalysis/195910

The Role of Technological Innovation in Shaping Investment Strategies in Emerging Markets: A Study on Risk and Return Dynamics

Yang Zeand Ooi Kok Loang (2025). *Unveiling Investor Biases That Shape Market Dynamics* (pp. 273-296).

www.irma-international.org/chapter/the-role-of-technological-innovation-in-shaping-investment-strategies-in-emerging-markets/365118

Applications of the Indigenous and Modern Career Counselling in Education

James N. Oigaraand Godrick E. Lyimo (2021). *Research Anthology on Navigating School Counseling in the 21st Century* (pp. 399-415).

www.irma-international.org/chapter/applications-of-the-indigenous-and-modern-career-counselling-in-education/281016

Theoretical Context of Cybercrime

Tansif Ur Rehman (2021). *Handbook of Research on Applied Social Psychology in Multiculturalism* (pp. 174-191).

www.irma-international.org/chapter/theoretical-context-of-cybercrime/281840

Smartphone Habits and Behaviour: A Review on Issues in Relation to the Physical and Psychological Well-Being of Users

Ida Haizatultasha Zaqreen, Sheirene Diana Hongand Nur Hayati Mohd Daud (2023). *Digital Psychology's Impact on Business and Society* (pp. 28-55).

www.irma-international.org/chapter/smartphone-habits-and-behaviour/315941