Information & Management 53 (2016) 91–108

Contents lists available at ScienceDirect

Information & Management

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

A model of emotion and computer abuse

Jongwoo (Jonathan) Kim [a,*], Eun Hee (Eunice) Park [b], Richard L. Baskerville [c]

[a] Management Science and Information Systems, University of Massachusetts Boston, 100 Morrissey Boulevard, Boston, MA 02125, United States
[b] Information Technology & Decision Sciences, Old Dominion University, 2072 Constant Hall, Norfolk, VA 23529, United States
[c] Computer Information Systems, Georgia State University, 35 Broad Street NW, Atlanta, GA 30302, United States

ARTICLE INFO

Article history:
Received 11 May 2013
Received in revised form 9 August 2015
Accepted 8 September 2015
Available online 25 September 2015

Keywords:
Information security
Computer abuse
Emotion process model
Abuse opportunity structure
Computer security behavioral factors

ABSTRACT

Internal computer abuse has received considerable research attention as a significant source of IS security incidents in organizations. We examine the effects of both organizational and individual factors on individuals' computer abuse intent. A theoretical model is developed based on two theories: abuse opportunity structure and emotion process. We empirically tested the model with 205 working professionals. We found that the abuse opportunity structure in organizations affects an individual's goal conduciveness, which in turn affects their abuse-positive affect. We also found that morality affects the abuse-positive affect, which in turn mediates the relationship between morality and abuse intent.

1. Introduction

More than 40% of security breaches are committed by disgruntled employees inside of an organization [26,28,103]. For example, insider misuse and unauthorized access to information by insiders have been identified as the top two security threats to businesses [128,149]. Current and former employees are the most frequent perpetrators of intellectual property theft, which costs US businesses more than $250 billion/year [113]. Even this reported statistic on insider abuse might be underestimated, as most organizations are reluctant to disclose such information because it could critically damage their reputation and business [36,97,103].

Prior studies have focused on the issue of compliance or noncompliance with IS security policies [6,115,137,138,149]. Assuming that employees are well intentioned, these studies have examined factors affecting compliance with security policies [15,31,63,116,151]. Although there are a small number of studies on insider threats [66,100,128], a majority of studies have examined the compliance issue in an attempt to maximize deterrence and prevention efforts. Keeney et al. [68] studied 49 cases of insider sabotage against information systems (IS). They found that in 83 percent of cases, grievances held by these perpetrators triggered criminal actions. Recent studies note that organizations need a more holistic approach that encompasses both the thought processes of the potential offender and the organizational context [148,149]. Our study fills this research gap.

To reduce insider abuse, understanding the psychological processes of disgruntled computer abusers within organizational structures is important [86]. *Computer abuse* refers to the "unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information systems by individuals" [125, p. 47]. Computer abuse is intricately linked to the psychological attributes of the abuser and to the organizational setting [73]. Prior research efforts have been focused on a control-function notion that is based on deterrence theory (DT). DT indicates that organizations should focus on various counter measures (e.g., security policies, security education, training, awareness programs, and monitoring) to deter computer abuse behavior. Such controls are known to be effective for limiting abuse [72]. For example, being aware of security sanctions and the severity of sanctions are found to be effective for reducing computer abuse [26].

Understanding and validating both organizational and individual factors and processes within an insider abuse context is crucial in the prevention of computer abuse. Prior studies of the relationship between the organizational setting and individual factors (e.g.) [146] suggest that they might have a significant impact on computer abuse behaviors. Ekblom [33] contends that explanations of how offenders interact with the settings in which a crime may or may not occur will help us better understand criminal behavior. The majority of prior studies on computer abuse

* Corresponding author. Tel.: +1 617 287 7746; fax: +1 617 287 7717.
E-mail addresses: jonathan.kim@umb.edu (J.(. Kim), epark@odu.edu (E.H.(. Park).

http://dx.doi.org/10.1016/j.im.2015.09.003
0378-7206/

have focused on cognition-based models [53,71,72,122]. These models have captured cognitional responses from the computer abuser and their influence on abuse behaviors. However, several prior studies [86,120] indicate that abuse behaviors such as sabotage and theft may involve emotional factors. Furthermore, recent case studies on computer abuse [9,83,90] have noted the critical presence of emotions as a psychological factor in computer abusers. There is a need to develop a framework that can predict the occurrence of emotions, along with cognitive factors, and explicate their consequences for computer abuse behaviors [116,118].

In this paper, we focus on investigating how organizational settings, such as the level of liberty and facilitation, affect employees' emotional processes and may lead potential abusers to computer abuse intent/behaviors. Our review of the literature in this area led us to identify the current limitations in the general understanding of how organizational and individual factors (such as emotions and morality) affect computer abuse intent and behaviors.

Our study aims to investigate and empirically validate how organizational settings and individual factors (i.e., emotional factors and morality) influence computer abuse intent. For this purpose, we develop a theoretical model based on a theory of computer crime opportunity structure [147] and on a theory of emotion process [43,44]. In the following section, we review related literature and develop a theoretical model. Then, we report our research methodology and our tests of the model using an experiment. Finally, we discuss our findings and present our contributions.

2. Literature review

2.1. Insider computer abuse

We conducted a literature review on insider computer abuse in the IS literature. Using security as a main keyword and carefully examining the articles, we collected 116 articles from top IS journals (over the period between 2007 and 2012) including *Decision Sciences, DSS, EJIS, ISR, JIS, JMIS, JAIS* and *MISQ.* We found thirteen articles using insider and threat as main keywords. Following this, a forward snowballing search turned up eighteen additional articles. The security orientation of IS research on insider computer abuse mostly follows a control-functional direction (see Appendix A). Such work includes security education and situational crime prevention techniques [146]. This work seeks to explain and justify security improvements through organizational factors and individual psychological factors.

Much of the past research has focused on the effectiveness of deterrent controls anchored to GDT within an organizational perspective (see Appendix A). Such research explores how managers can create effective deterrence policies by being aware of effects and alternative behaviors [123]. These prior studies show that such controls are effective deterrents. The focus of the study of internal abuse has evolved from organizational factors to individual factors and the combination of both as shown in Appendix A. Prior studies on individual factors have focused on cognitive and rational factors. For instance, recent studies on insider abuse identified individual factors such as policy awareness and self-efficacy. In particular, the internal perceptions of potential abusers, especially with regard to organizational deterrence policies, have proved significant for limiting abuse [72]. In addition, ensuring that potential abusers are aware of policies and the severity of sanctions has also been found to be effective for limiting abuse [26].

Our study is motivated by the need for research focusing on both organizational and individual factors, particularly factors related to emotion. While the psychological effects of controls on organizational computer users are important, a more comprehensive understanding will emerge from situating the psychological process of a potential computer abuser within the context of their organizational setting. A recent study [149] identified the important role of emotion. By expanding the scope of a security study to include an organization-centric component and an individual-centric component (particularly including emotion), we can grasp both the situation in which the individual is embedded and the psychological process that ensues. To achieve this goal, we develop an integrated computer abuse model that incorporates both an organization-centric component and an individual-centric component that incorporates emotion. Then, we empirically test the model. In the following section, we explain the emotion process model.

2.2. Emotion process model

To explain computer abuse behaviors, we draw on the study of emotion [8,59], which suggests two approaches: a discrete emotion approach and a componential approach. The componential approach focuses on the components related to emotional experience and their relationships. Much of the IS emotion research (e.g.) [10,14,63,139] has employed a discrete emotion approach that focuses on a small set of fundamental emotions such as anger, fear, shame, guilt, happiness, and joy [8,60,91,131]. This approach enables researchers to explore the causality between emotion and cognition [60]. However, it also limits the analysis of emotion to a few defined sets of basic emotions [89] instead of taking a holistic view of emotion processes. This focus on discrete emotions in IS research suggests that the IS field has only a partial understanding of the emotion processes.

Our study follows a componential approach that situates emotion as a process (e.g.) [3,34,38,59]. Each component (for example, event, appraisal, action readiness, etc.) of the emotion process influences the others as shown in Fig. 1 [43,84]. Instead of limiting the investigation to a particular discrete emotion, this approach decomposes emotional experiences into detailed components (e.g., [43,44,89,111]). It provides a broad set of emotions defined by various types of appraisals [59]. This approach also benefits researchers by permitting a systematic and detailed explanation of how emotions are shaped and interact [89].

Fig. 1 shows an emotion process model adapted from Frijda [42–44], which employs the componential approach and provides

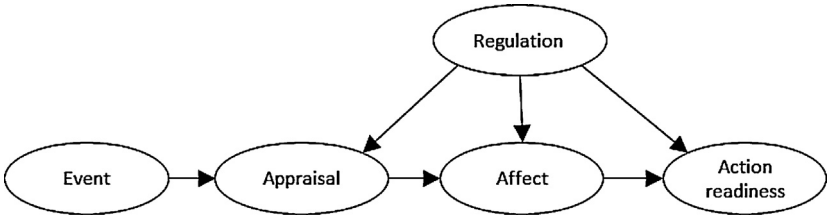

Fig. 1. The central emotion process model [42–44]. Note: It represents an adapted emotion process model and shows key components relevant to our research.