Information & Management 52 (2015) 1012–1024

Contents lists available at ScienceDirect

Information & Management

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

Dysfunctional information system behaviors are not all created the same: Challenges to the generalizability of security-based research

Hadrian Geri Djajadikerta [a,*], Saiyidi Mat Roni [a], Terri Trireksani [b]

[a] School of Business, Edith Cowan University, 270 Joondalup Drive, Joondalup, WA 6027, Australia
[b] School of Management and Governance, Murdoch University, 90 South Street, Murdoch, WA 6150, Australia

ARTICLE INFO

Article history:
Received 12 April 2014
Received in revised form 5 June 2015
Accepted 15 July 2015
Available online 23 July 2015

Keywords:
Dysfunctional behavior taxonomy
Theory of planned behavior
Behavioral intention
Structural equation modeling
Partial least square
Vignettes

ABSTRACT

Conflicting findings in the existing studies on insider dysfunctional information system (IS) behaviors have led some researchers to raise methodological concerns that samples in these studies are aggregated or disaggregated without sufficient attempt to differentiate their fundamental differences. Using a four-quadrant behavior taxonomy, this study investigates different types of dysfunctional information system behaviors to determine if, among them, there are any differences in behavioral intentions and in the causal links between these intentions and their predictor variables. The results show that both the intentions and the causal links between these intentions and their predictors vary among the four behavior categories.

1. Introduction

Information system (IS) security risks posed by the inappropriate actions of individual members of an organization have been a topic of interest in a vast amount of literature [57,101,103]. These individuals are insiders who sit behind the organizational firewall and are empowered with escalated user privileges [107]. They have a dual role in information security systems, both as allies and as a source of threats [99]. Studies have suggested that within the information security chain, insiders remain the weakest link in the effort to secure organizational IS assets [28,101,103,110]. Some surveys and investigations have also shown that despite rapid advancement in protection technologies as well as IS security policies and procedures, IS security breaches remain significant, and they are substantially linked to the actions of insiders [9,85].

Calls for more studies on the behavioral aspects of IS security have long been voiced [107], and there are some significant studies in this area. The studies in the IS security area that look into the behavioral aspects of insiders have provided insights into the effects of insider dysfunctional behavior on organizational IS assets. These can be seen in valuable work on IS security compliance/non-compliance behavior [15,22,44,55,56,60,71,79,88,93,102] including motivations to comply with IS security policies [59,72,94,91], IS misuse [10,33,43,54,77,92,103,109], and studies on computer abuse [73,75,81]. These IS security studies, however, have largely focused on non-malicious and policy non-compliance behavior [107,110]. Thus, there is a need to address a broader range of actions that pose various levels of risk to organizational IS assets.

The following are some examples of the above studies. Myyry et al. [79] aimed to explain employee IS non-compliance in terms of moral reasoning and values. Hu et al. [56] described and tested a model of information security policy violation based on multiple criminological perspectives. Ifinedo [59] integrated social bonding, social influence, and cognitive processing perspectives to understand employee IS security policy compliance behavior. Son [94] attempted to explain why employees do or do not follow IS security rules using an intrinsic motivation model. Lowry et al. [73] used fairness theory and reactance theory to explain why employees may blame organizations for and retaliate against improved IS policies.

In general, these studies can be aggregated as studies of IS security deviant behavior within the context of volitional malicious and non-malicious behavior [22,17,110]. This aggregated behavior typology, despite its usefulness, does not differentiate similar yet fundamentally disparate behavior. For example, intentional IS record modifications within one's authorized workspace require

* Corresponding author at: Edith Cowan University, 270 Joondalup Drive, Joondalup WA 6027, Australia. Tel.: +61 8 6304 5353.
E-mail addresses: h.djajadikerta@ecu.edu.au (H.G. Djajadikerta), m.matroni@ecu.edu.au (S.M. Roni), t.trireksani@murdoch.edu.au (T. Trireksani).

http://dx.doi.org/10.1016/j.im.2015.07.008
0378-7206/

fewer computer skills, while record changes requiring escalated user privilege require more computer knowledge to penetrate the internal firewall and to remove the digital footprint of such actions from log records. Consequently, control remedies such as instituting supervisory authorization prior to record changes do not fully address the act of unauthorized record changes that require computer competency, which calls for protective control technologies to detect such attempts. The deviant behavior perspective therefore provides a foundation to understand negative insider behavior at the aggregated level but fails to address typological differences at the subset level as behavior is categorized only on the basis of intentions (i.e., malicious and non-malicious).

Consequently, investigating insider dysfunctional behavior without applying an appropriate segregation of behavior categories could lead to sample contamination, which limits the practical use of such studies. Crossler et al. [28], and Posey et al. [82] have raised such methodological concerns, indicating that studies that placesole emphasis on improving security awareness among insiders do not address issues related to insiders who engage in acts driven by malicious intentions. This is "because knowledge created from a focus on a single behavior or subset of behaviors does not necessarily generalize to the grand structure of behaviors" [82, p. 1190]. Their concerns are in line with Guo [46] and D'arcy and Herath's [32] suggestions that the studies in security-related behavior in IS occasionally report inconsistent and contradictory results. The disparate findings were partly the result of a diverse conceptualization of such behaviors, in which "many of the concepts overlap with each other on some dimensions and yet are different on others" [46, p. 242], and partly because factors explaining IS security compliance do not necessarily account for policy violations [46].

Taking the above discussion into consideration, this study addresses this gap in the literature and attempts to provide an indication of how dysfunctional information system behavior at the aggregated and subset levels plays a crucial role in information system security (mis)behavior. Overall, this paper searches for differences in behavioral intentions and in the cause–effect relationships between these intentions and their predictor variables among different types of dysfunctional information system behavior. This paper accordingly addresses the above methodological issues in the current studies on insider dysfunctional behavior in information systems (e.g., Refs. [28, 32, 46, 83, 107]), allowing an examination of behavioral intentions and changes in the predictors of these intentions across different types of dysfunctional behavior.

The next section of the paper reviews conceptual discussions regarding dysfunctional information system behavior, categories of insider behavior based on Stanton's et al. [95] taxonomy, intentions of dysfunctional behavior, and the antecedents of intention. This conceptual discussion leads to the development of research propositions, which are subsequently described. This is followed by a presentation of the research methodology and data employed in this study. This study uses vignettes in a survey of middle managers of medium sized enterprises (SMEs) and tests the model and analyzes the responses using partial least square structural equation modeling (PLS-SEM). A description and discussion of the empirical results follow, where the study provides important findings indicating that both the intentions and the causal links between these intentions and their antecedents vary among different behavior categories. This paper concludes with a summary, limitations and future research opportunities that emerge from the study.

2. Conceptual discussion and proposition development

Attempts to disaggregate seemingly similar behavior have been demonstrated by Davis [36], who modeled two pathological internet uses/misuses with reference to their symptoms and effects. The work not only provides a general foundation for dysfunctional behavior classifications but also offers some understanding of how intricate connections of psychopathology (e.g., depression and social anxiety) and situational factors reinforce Internet users' cognitive approaches, leading to Internet uses/misuses. Magklaras and Furnell [76] extended this concept by including computer skills as part of their proposed user sophistication model, which advanced the identification and classification of dysfunctional behavior.

Stanton et al. [95] proposed that the dysfunctional behavior of interest should be mapped onto a two-dimensional plane, the *x*-axis being the intensity of intentions (i.e., malicious to neutral to benevolent) and the *y*-axis being the level of computer skills required (i.e., low to high). Using this 2-vector plane, Stanton et al. [95], in their study, listed 94 types of behavior that were later categorized into 6 types of behavior, which include 4 risky types of insider behavior (i.e., *intentional destruction*, *detrimental misuse*, *dangerous tinkering*, and *naïve mistake*) and 2 types of behavior that are considered acceptable practices (i.e., *aware assurance* and *basic hygiene*). Their work is one of a number of significant studies that have paved the way to aggregation and disaggregation of insider behavior. These 6 types of behavior are shown in Fig. 1 and summarized in Table 1.

Recently, Guo [46] suggested eight indicators to identify the subsets of dysfunctional behavior: (1) intentions (focuses on volitional/non-volitional action), (2) malicious/non-malicious, (3) level of computer skills and knowledge, (4) types of perpetrator, (5) job relatedness, (6) direct or indirect damage to organizations, (7) requiring action or absence of action by employees, and (8) actions are subject to policies.

To clearly address the insider dysfunctional behavior perspective in the existing studies, the relevant literature was analyzed to see how thematic behaviors were studied, how different types of behavior were pooled together and/or separately examined, and where these behaviors reside within Stanton et al.'s [95] taxonomy (see Appendix A). The information in Appendix A highlights the general concerns raised by Crossler et al. [28], Posey et al. [82], Guo [46], Warkentin and Willison [107], and D'arcy and Herath [32] regarding the methodological issues in the existing studies on insider dysfunctional behavior, particularly where samples are aggregated or disaggregated with limited or no attempt to differentiate their fundamental differences.

2.1. Using intention to capture dysfunctional behavior

Intention has been recognized as a good predictor of actual behavior [1,4,20], driving a person to behave the way he/she does. The essence of the intention–behavior relationship is that the stronger the intention a person has, the more likely it is that the person will engage in the behavior [104,112]. Intention is "assumed to capture the motivational factors that influence a

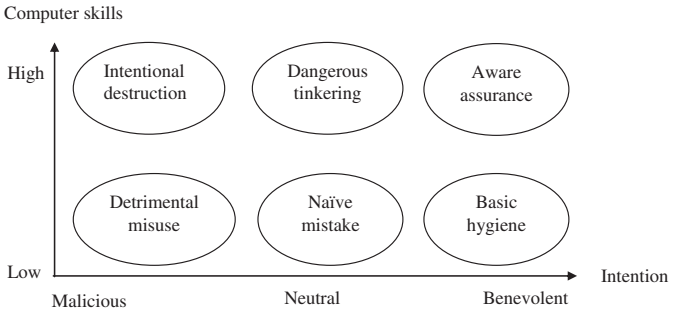

Fig. 1. Insider behavior categories [95].