Decision Support Systems 66 (2014) 93–101

Contents lists available at ScienceDirect

Decision Support Systems

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

Development and validation of instruments of information security deviant behavior

Amanda M.Y. Chu [a], Patrick Y.K. Chau [b,*]

[a] Department of Management Sciences, The City University of Hong Kong, Hong Kong
[b] Faculty of Business and Economics, The University of Hong Kong, Hong Kong

ARTICLE INFO

Article history:
Received 11 July 2013
Received in revised form 6 June 2014
Accepted 10 June 2014
Available online 19 June 2014

Keywords:
Information security
Deviant behavior
Instrument development
Measurement
Validity
Reliability

ABSTRACT

Information security deviant behavior (ISDB) of employees is a serious threat to organizations. However, not much empirical research on ISDB has been carried out. This paper attempts to develop and validate instruments of ISDB using an empirical method. Two instruments of ISDB are proposed and tested, including a four-item instrument of resource misuse (ISDB that is related to the misuse of information systems resources) and a three-item instrument of security carelessness (ISDB that is related to the employees' omissive activities when using computers or handling data). A rigorous instrument development process which includes three surveys and addresses six crucial measurement properties (content analysis, factorial validity, reliability, convergent validity, discriminant validity, and nomological validity) is adopted. The implications of these two instruments for future empirical studies on ISDB are discussed.

1. Introduction

Information security deviant behavior (ISDB) of employees, such as leaving removable storage devices unattended and using untrusted applications at work, is a serious threat to organizations. A recent survey reported that 63% of interviewed information security professionals deemed employees to be a high concern for organizations; the percentage was higher than that of hackers (55%) or organized crime (38%) [24]. ISDB also results in serious financial losses for organizations, with a 2009 security survey reporting the average annual such losses arising from security incidents to be US$234,244 per company [59]. A quarter of respondents to this survey believed that at least 60% of these financial losses stem from insiders' actions.

Despite the increasing prevalence and high associated costs of ISDB in the workplace, our understanding of this topic remains limited and fragmented [30,64,78]. The lack of instruments to measure ISDB presents a barrier to our understanding of the relationship between ISDB and correlated constructs and the development of theories and frameworks to tackle security problems [48]. In order to understand ISDB, it is important to develop reliable and valid instruments to measure it. This study aims to fill this research gap by developing instruments for the measurement of ISDB under a rigorous instrument development process. The instruments developed are useful for researchers to investigate the different properties of such behavior.

The remainder of this paper is organized as follows. We review related studies and discuss the background theory in Section 2, and then describe how we used a four-stage process to develop the instruments for ISDB in Sections 3 and 4. Section 3 focuses on the domain specification, instrument development and instrument refinement while Section 4 focuses on the instrument validity. Finally, we discuss the implications of the findings and draw our conclusion in Section 5.

2. Background theory

2.1. Information security deviant behavior

Workplace deviant behavior is not a new concept. A number of studies in sociology, psychology, and organizational behavior have attempted to study acts related to workplace deviant behavior and used different terminologies to denote the behavior. Examples include antisocial behavior [26], counterproductive workplace behavior [44], organizational misbehavior [74], organizational retaliation behavior [65], workplace aggression [47], and workplace deviance [60]. Regardless of the different terminologies, prior literature tended to vary workplace deviant behavior based on its target — interpersonal deviance and organizational deviance. Table 1 summarizes the definitions of different terminologies used to describe the behavior and examples on interpersonal deviance and organizational deviance in each terminology. Interpersonal deviance was further categorized into political deviance and personal aggression as well as organizational deviance into property deviance and production deviance [60].

* Corresponding author. Tel.: +852 3917 1025.
E-mail address: pchau@business.hku.hk (P.Y.K. Chau).

http://dx.doi.org/10.1016/j.dss.2014.06.008
0167-9236/© 2014 Elsevier B.V. All rights reserved.

Table 1
Definitions of different terminologies to describe workplace deviant behavior.

Construct	Definition	Two examples on organizational deviance	Two examples on interpersonal deviance
Antisocial behavior [26]	Any behavior that brings harm, or is intended to bring harm, to an organization, its employees, or stakeholders (p. vii)	Sabotage; violations of confidentiality	Violence; sexual harassment
Counterproductive workplace behavior [44]	Behavior by an organizational member that results in harming the organization or its members (p. 37)	Volitional absenteeism; drug and alcohol abuse	Violence; spreading rumors
Organizational misbehavior [74]	Acts in the workplace that are done intentionally and constitute a violation of rules pertaining to such behavior (p. 3)	Vandalism and sabotage; substance abuse on the job	Sexual harassment; bullying
Organizational retaliation behavior [65]	Adverse reaction to perceived unfairness by disgruntled employees towards their employer (p. 434)	Wasting company materials; calling in sick when not ill	Gossiping about his or her boss; spreading rumors about coworkers
Workplace aggression [47]	Any form of behavior by which individuals attempt to harm others at work or their organizations (p. 393)	Failure to return phone calls or respond to memos; intentional work slowdowns	Giving someone the silent treatment; verbal sexual harassment
Workplace deviance [60]	Voluntary behavior of organizational members that violates significant organizational norms and, in so doing, threatens the well-being of the organization and/or its members (p. 7)	Taking property from work without permission; coming in late to work without permission	Making fun of someone at work; saying something hurtful to someone at work

Workplace deviant behavior has been investigated from various theoretical perspectives. For example, O'Leary-Kelly et al. [50] developed a framework and identified sets of antecedents in terms of individual and organizational environment characteristics using social learning theory [2]. Martinko et al. [44] further expanded the framework by considering attribution theory [76] and causal reasoning process. Some theories may be more appropriate to explain specific type of workplace deviant behavior. For instance, self-interest and role conflict may be more applicable to explaining lying in organizations [28] while identity theory may be more useful to explain employee alcohol use and illicit drug use [23].

Traditionally, workplace deviant behavior seldom took information systems or technology into consideration. As a result, the measures and models developed for the constructs therein may be unsuitable for a consideration of ISDB because the nature of traditional workplace deviance discussed in the prior literature (in which the actor reveals his or her identity, and a computer is not necessarily involved) and ISDB (in which the actor is dependent on a computer and can hide his or her identity) differs considerably. For example, in our previous discussion, researchers tended to classify the workplace deviant behavior into interpersonal deviance and organizational deviance but interpersonal deviance may not be applicable when we examine ISDB. Another example is that many of previous studies in workplace deviant behavior assumed intentionality (e.g., Refs. [44,51,74]). However, ISDB is a voluntary behavior rather than an intentional behavior.

With organizations' widespread adoption of computers and networks, workplace deviant behavior is no longer restricted to physical actions and direct harm to the organization or its members, but may include threats to information security on organizational computer systems. Little empirical research to date focuses on understanding deviant employee behavior that threatens information security within organizations because of the sensitive nature of the topic [36] and the absence of valid instruments [69]. Therefore, ISDB concept remains underdeveloped. To enhance academic discipline growth, it is important to define differentiating constructs for ISDB and to identify their instruments clearly and systematically. ISDB varies along a continuum of dimensions and can be explained by a typological theory [13]. One of the dimensions to organize ISDB is frequency and found that two common types of ISDB are misuse of information systems resource (resource misuse) and information security careless (security carelessness). Resource misuse is related to the misuse of any information systems resources including applications, the Internet, and networks in the workplace, while security carelessness involves employees' omissive activities when using computers or handling data in daily operations. The nature of resource misuse and security careless is different. Our target is to validate and test instruments of ISDB that can be commonly found in the workplace and in a variety of industries and occupations using an empirical method. Therefore, in this study, we attempt to develop instruments to measure resource misuse and security carelessness. In order to create instruments for ISDB for application in a variety of industries and occupations, we integrate knowledge from the literature with industry wisdom. As Chiasson and Davidson [12] stated, “Industry provides an important contextual “space” to build new IS theory and to evaluate the boundaries of existing IS theory” (p. 591).

2.2. Decision support for information security management

Organizations are increasingly dependent on computers, rendering information security management a crucial organizational concern [21,41]. Researchers suggest that information security is not only a technical or economic issue but also a human one and that is of concern not only to management but to everyone in the organization [34,64]. Mahmood et al. [42] emphasized that “without a better and truer understanding of the antisocial behavior that prompts individuals to attack computer systems, we cannot readily design the most effective countermeasures” (p. 432). Some previous works have attempted to examine specific types of deviant workplace behavior in information security such as software piracy [53] and nonwork-related computing [6]. However, the understanding of ISDB, which is a major source of computer systems security risk and necessary component on the foundation for designing DSS for security decision making and planning in organizations, is still not clear [79]. One possible explanation of the shortage of the research is the difficulty in measuring the behavior. The availability of validated instruments of ISDB may be useful for facilitating the much-needed empirical research for the behavior so as to provide efficiency of decision support for proper security strategy and controls implemented within organizations. The aim of this study is to produce such instruments.

3. Instrument development

Churchill [14] provided a methodological guide used in instrument development and recommended a paradigm for instrument development comprising three stages: 1) definition and specification of the construct domain, 2) generation of items for the specified domain, and 3) instrument refinement. Many MIS research that addressed instrument development and process highlighted the importance of instrument validation (e.g., Refs. [35,69]) and therefore, suggested that instrument development usually include three steps, including item creation, instrument development, and instrument testing [45]. To further emphasize on the instrument validation, Lewis et al. [40] addressed that a quality measurement instrument should achieve an adequate level of construct validity which includes content validity, factorial validity, reliability, convergent validity, discriminant validity, and nomological validity. Based on the previous recommendations on