Computers in Human Behavior 38 (2014) 220–228

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory

Lijiao Cheng [a,*], Wenli Li [a], Qingguo Zhai [b], Russell Smyth [c]

[a] Faculty of Management and Economics, Dalian University of Technology, Dalian, Liaoning 116023, China
[b] The Faculty of Business, Federation University Australia, Ballarat, Vic., Australia
[c] Department of Economics, Monash University, Clayton, Vic., Australia

ARTICLE INFO

Article history:
Available online 1 July 2014

Keywords:
Deterrence theory
Neutralization theory
Personal use of the Internet

ABSTRACT

This paper examines the influence of neutralization techniques, perceived sanction severity, perceived detection certainty and perceived benefits of using the Internet for personal purposes on intention to use the Internet at work for personal use. To do so, we draw on a conceptual framework integrating neutralization theory and general deterrence theory. The study finds that both neutralization techniques and perceived benefits have a positive effect on personal use of the Internet. Perceived detection certainty is found to have a negative effect on personal use of the Internet, while the effect of perceived sanctions severity on personal use of the Internet is not significant. The effect of neutralization and perceived benefits are much stronger than perceived detection certainty. The findings suggest that people may think more about neutralization and perceived benefits than they do about costs, when deciding whether to use the Internet at work for personal purposes.

1. Introduction

Personal use of the Internet refers to the use of the Internet for personal, non-work purposes during scheduled work time (Moody & Siponen, 2013). These non-work-related activities include visiting news sites, downloading files for personal purposes, engaging in personal e-commerce, online social networking, personal communication, or even committing cybercrimes (Kim & Byrne, 2011; Moody & Siponen, 2013; Ugrin & Pearson, 2013). Researchers have noted that personal use of the Internet can be detrimental to organizations (Blanchard & Henle, 2008; Bock & Ho, 2009; Case & Young, 2002; Garrett & Danziger, 2008a; Jia, Jia, & Karau, 2013; Lim, 2002; Lim & Chen, 2012; Moody & Siponen, 2013; Young, 2011). To be specific, these are at least four potential costs to organizations of personal Internet use. First, personal use of the Internet can decrease employee productivity. Second, personal use of the Internet can result in bandwidth degradation and network congestion. Third, personal use of the Internet can result in threats to the security of corporate data. Specific risks associated with personal use involve downloads leading to malware and spyware infections, such as rootkits, spamware, viruses, Trojan horses and worms as well as browser hijacking (e.g. SnapDo). Fourth, personal use of the Internet can put organizations at risk of legal liability if employees engage in illegal activities while using the Internet.

To cope with the epidemic of personal use of the Internet within the workplace, many organizations have set up Internet use policy and control mechanisms (Siau, Nah, & Teng, 2002; Young, 2010), conducted management training (McBride, Carter, & Warkentin, 2012; Young & Case, 2004), and monitored employees' Internet usage (Kankanhalli, Teo, Tan, & Wei, 2003; Mirchandani, 2004; Posey, Bennett, Roberts, & Lowry, 2011). The personal use of the Internet has also attracted the interest of several researchers who have considered various aspects of this issue (see e.g. Lim & Chen, 2012; Mirchandani, 2004; Mirchandani & Motwani, 2003; Moody & Siponen, 2013; Ugrin & Pearson, 2008; Ugrin & Pearson, 2013).

The aim of this study is to examine the effect of neutralization, perceived detection certainty, perceived sanctions severity and perceived benefits of using the Internet for personal purposes on the intention to use the Internet at work for personal use. To do so, we provide a conceptual framework, drawing on neutralization and general deterrence theories. Neutralization theory postulates that individuals try to convince themselves, and others, that their deviant behavior is justifiable. It represents a priori rationalization that individuals employ in order to convince themselves that deviant behavior is excusable (e.g. Lim, 2002; Sykes & Matza, 1957). Lim (2002) develops a specific neutralization technique called the 'metaphor of the ledger', which entails the individual

[*] Corresponding author. Tel.: +86 411 84708058; fax: +86 411 84708342.
E-mail addresses: imchenglijiao@gmail.com (L. Cheng), wlli@dlut.edu.cn (W. Li), q.zhai@federation.edu.au (Q. Zhai), russell.smyth@monash.edu (R. Smyth).

http://dx.doi.org/10.1016/j.chb.2014.05.043
0747-5632/© 2014 Elsevier Ltd. All rights reserved.

convincing himself or herself that he or she has accumulated enough points on the positive side of the ledger to justify engaging in deviant behavior on the negative side of the ledger. The 'metaphor of the ledger' has its origins in social exchange theory, which posits that employees seek a balance in their exchange relationships with organizations (Blau, 1964). If employees have behavioral 'credits', they can 'cash' these through engaging in poor behavior. At the same time, if the individual perceives the organization has treated them poorly, social exchange theory suggests that individuals can feel justified in reciprocating through engaging in behavior contrary to the organization's interests.

Deterrence theory is premised on the notion that individuals respond to incentives and that greater deterrence in the form of a higher probability of detection and more severe sanctions will curtail personal Internet use (Ugrin & Pearson, 2013).

We extend the existing literature in four ways. First, scant research has examined the personal use of the Internet within the context of neutralization theory. Existing research has only looked at the effect of one sub-dimension of neutralization on the personal use of the Internet (Lim, 2002). We extend this research to include five sub-dimensions of neutralization.

The second contribution of the study is that we extend general deterrence theory by incorporating benefits into the model. Existing studies within the context of deterrence theory have mainly focused on the cost to individuals, while the benefits to individuals have been neglected (Vance & Siponen, 2012). Two exceptions are studies by Moody and Siponen (2013) and Pee, Woon, and Kankanhalli (2008).

The third contribution is that we integrate both deterrence and neutralization theories to study the personal use of the Internet. To our knowledge, no research exists on the personal use of the Internet, drawing on both general deterrence theory and neutralization theory. Integrating neutralization theory and general deterrence theory can provide a more complete picture for understanding personal use of the Internet. According to Willison and Warkentin (2013), individuals may attempt to justify and rationalize anti-organizational behavior using appropriate neutralization techniques. Siponen and Vance (2010), in their study of information systems (IS) security, argued that employees' violation of IS security is not always best explained by fear of sanctions. The reason is that employees may use neutralization techniques; rationalizations which allow them to excuse, or justify, the perceived harm of violation of organization policies. This argument can also apply to the personal use of the Internet (Siponen & Vance, 2010).

The fourth contribution is in terms of our geographic focus on the personal use of the Internet in China. Most extant research on the personal use of the Internet has been conducted in specific western countries (Moody & Siponen, 2013; Ugrin & Pearson, 2008; Ugrin & Pearson, 2013). To this point, there is a dearth of studies on the personal use of the Internet in China. Because of myriad cultural differences, research findings in the west may not be necessarily generalizable to China.

The results will be of interest to management and information security in companies with employees who use the Internet, as well as information security and organizational behavior scholars interested in studying personal use of the Internet at work. The results for the deterrence variables will also be of interest to scholars in other fields, such as criminology and economics as a specific application of the relative effect of the certainty of apprehension and severity of punishment on personal use of the Internet in the workplace.

The remainder of the paper is set out as follows. The next section gives an outline of neutralization theory, general deterrence theory as well as presenting our hypotheses. We then outline the data and research method. This is followed by presentation, and discussion of the results. The final section of the paper details limitations of the study and implications for research and for practice.

2. Conceptual framework and hypotheses

2.1. Neutralization techniques

Neutralization techniques refer to rationalizations which individuals invoke to convince themselves, and others, that their deviant behaviors are justifiable and/or excusable (Lim, 2002; Sykes & Matza, 1957). Individuals use these strategies to reconcile the discrepancies between their deviant behavior and the positive self-image that they wish to project. According to Willison and Warkentin (2013), neutralization theory may be particularly worthy of study in the corporate context, as corporate employees are far more susceptible to feelings of guilt and shame, relative to career criminals. Recently, organizational scholars have started to use neutralization techniques to understand workplace deviance, such as the personal use of the Internet (Lim, 2002; Rajah & Lim, 2011) and IS security policy violations (Siponen & Vance, 2010; Willison & Warkentin, 2013).

Sykes and Matza (1957) proposed five techniques of neutralization; namely, denial of responsibility, denial of injury, denial of victim, condemnation of the condemners and appeal to higher loyalties. Denial of responsibility entails a person committing a deviant act placing the blame on an alternative source or circumstance (Siponen & Vance, 2010). The perpetrator convinces himself, or herself, that he, or she, is not really liable due to 'factors beyond their control' which causes their deviant activity (Harris & Dumas, 2009). Denial of injury involves justifying an action on the basis that it is victimless or that it causes little, or no, harm (Sykes & Matza, 1957). Using denial of injury, the individual may claim that the personal use of the Internet does not harm organizational property or inflict harm on other individuals. Denial of victim entails claiming that the deviant act can be justified because the victim deserved whatever happened. Condemnation of the condemners occurs when a person committing a deviant act criticizes those who condemn them in an attempt to shift the blame. With appeal to higher loyalties, a person committing a deviant act seeks to justify their behavior as being for the greater good, with long term benefits that justify their actions. Following Siponen and Vance (2010) these five dimensions are conceptualized as a type two second-order construct (Jarvis, Mackenzie, Podsakoff, Mick, & Bearden, 2003), which is formatively composed of reflective sub-constructs.

According to Willison and Warkentin (2013), deviant corporate employees are likely to draw on techniques of neutralization in an attempt to avoid feelings of guilt. There is also empirical evidence to show that neutralization is correlated with intention to engage in deviant acts, such as intention to violate information security policy (Siponen & Vance, 2010). The same mechanism seems applicable to employee's personal use of the Internet. Therefore, the following hypothesis is proposed.

H1. Employees' usage of neutralization techniques will be positively related to their intention to use the Internet for personal purposes.

2.2. General deterrence theory

General deterrence theory (GDT) was originally developed as a mechanism to reduce the extent to which people engage in deviant behavior. It rests on the proposition that human behavior is to some degree rational, and therefore can be influenced by incentives, particularly the negative incentives inherent in formal