COPYRIGHT NOTICE

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

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.

Keywords: Deterrence theory; Neutralization theory; Personal use of the Internet.

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, et al., 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

* Corresponding author: Lijiao Cheng at Faculty of Management and Economics, Dalian University of Technology, Dalian, Liaoning, China, 116023. Tel.: +86 411 84708058; fax: +86 411 84708342.

E-mail addresses: imchenglijiao@gmail.com (Lijiao Cheng), wlli@dlut.edu.cn (Wenli Li), q.zhai@federation.edu.au (Qingguo Zhai), russell.smyth@monash.edu (Russell Smyth)

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, et al., 2002; Young, 2010), conducted management training (McBride, et al., 2012; Young & Case, 2004), and monitored employees' Internet usage (Kankanhalli, et al., 2003; Mirchandani, 2004; Posey, et al., 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 & Motwani, 2003; Mirchandani, 2004; 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 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 et al. (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, et al., 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 sanction (Wenzel, 2004). GDT suggests that the threat of sanctions can modify employee actions when the potential punishment is weighed against the potential

benefit of a specific behavior (Ugrin & Pearson, 2013). GDT has previously been used in research on the personal use of the Internet (Mirchandani & Motwani, 2003; Mirchandani, 2004; Moody & Siponen, 2013; Ugrin & Pearson, 2008; Ugrin & Pearson, 2013). In our study, we extend GDT to incorporate the benefits of the personal use of the Internet. The costs of the personal use of the Internet include the possibility of detection and severity of sanctions. Perceived benefits of the personal use of the Internet include saving money and time, convenience of use and emotional benefits such as making work life more enjoyable (Li, et al., 2010).

2.2.1. Sanctions and the personal use of the Internet

Sanctions include perceived sanction severity and perceived detection certainty. Sanction severity refers to an individual's belief that their deviant behavior will be harshly punished, while detection certainty refers to the probability that they will be caught. According to GDT, individuals who perceive that the probability of detection and severity of punishment is higher will be less likely to engage in deviant behavior. Hence,

H2: Sanction severity will be negatively related to employees' intention to use the Internet for personal purposes.

H3: Detection certainty will be negatively related to employees' intention to use the Internet for personal purposes.

2.2.2. Perceived benefits and the personal use of the Internet

Perceived benefits refer to the overall expected benefits that an employee could obtain from the personal use of the Internet. The benefits can include one or more of saving time or money, convenience or enjoying a more interesting work life (Li, et al., 2010; Lim & Chen, 2012; Moody & Siponen, 2013; Pee, et al., 2008). Convenience is perceived to be a significant benefit of the personal use of the Internet. Some employees also use the Internet for entertainment purposes such as downloading movies, gaming and social networking (Johnson & Indvik, 2004; Pee, et al., 2008). These perceived benefits may override the impact of sanctions, and lead to use of the Internet for personal purposes. Therefore,

H4: Perceived benefits will be positively related to employee intention to use the Internet for personal purposes.

2.3. Control variables

Extant research has found that variables such as age (Vitak, et al., 2011), gender (Chen, et al., 2011) and education level (Garrett & Danziger, 2008b) can impact the personal use of the Internet. These variables are employed as control variables in this study.

3. Research method

3.1. Instruments

All the constructs were measured with previously validated instruments. Personal use of the Internet was measured with the corresponding instrument of Pee, et al. (2008), perceived benefits, detection certainty and sanction severity were measured in the same manner as in Li, et al. (2010). Denial of responsibility, and denial of injury were measured with the items from Siponen and Vance (2010). Denial of victim is from Morris and Higgins (2009). Condemnation of the condemner was from the items in Buzzell (2005). Appeal to higher loyalties was from the instrument of Hinduja (2007). All items were measured on a seven-point Likert scale, in which 1 denoted "strongly disagree" and 7 denoted "strongly agree".

As the current study was conducted in a Chinese speaking context, and the original measures of the studied constructs were developed in English, the survey instrument was translated from English into Chinese following the procedure recommended by Brislin (1993). First, the instruments were translated from the original English into Chinese and subsequently back translated into English by another bilingual. The back translated text was then compared with the original text. In instances in which discrepancies existed, the Chinese version and the original English version were examined and, if necessary, the final translation was amended.

Before administration of the survey, the questionnaires were distributed to 50 middle-level managers at five Dalian companies for their feedback and some revisions were made based on their feedback. The items are shown in Table 4.

3.2. Sample and procedures

The target population was employees working in organizations with Internet use policies. Data were collected in 2012 mainly from employees working in telecommunication and financial institutions. Each of the organizations had Internet use policies which explicitly stated that no personal use of the Internet is allowed. In each case the Internet use policy states that individuals violating the policy will be sanctioned. The sanctions are of differing severity up to, and including, termination. For companies in Dalian, we collected data from five organizations with Internet use policies. We distributed 200 paper edition questionnaires to employees in these five companies and received 118 completed questionnaires. Specifically, one of the authors visited each of the organizations in Dalian, distributed the questionnaires to the selected respondents and collected the questionnaires immediately after completion. For companies outside Dalian, we collected data via an on-line survey using a professional survey website. Specifically, we sent e-mails with a hyperlink to the survey to 500 people working in organizations which have an Internet use policy prohibiting personal use, inviting them to participate in the online survey. We received 112 completed questionnaires from the online survey. Most of the respondents to the online survey were from telecommunication companies and financial institutions. Altogether, we collected 230 completed questionnaires.

The characteristics of the respondents are reported in Table 1. Table 1 indicates that the proportion of men was a little higher than women and most of the respondents were aged between 19 and 35 years old. About three-quarters of the respondents have

a bachelor degree or above. About three-quarters of the respondents had worked in their current companies for less than 3 years. About 70% of the respondents use computers more than 6 hours a day. There is no general information about the characteristics of corporate employees in China as a whole, so we cannot compare our sample with the characteristics of corporate employees as a whole to assess the representativeness of our sample. However, our sample is similar to other IS security studies in China in terms of age, education and gender (Hu, et al., 2011).

[Insert Table 1 about here]

Some of the responses were collected through a paper survey and others through an online survey. Meta-analyses suggest that while the response rates differ between online and paper surveys, representativeness is often similar (Cook, et al., 2000). Table 2 compares the characteristics of respondents to the paper survey and respondents to the online survey in terms of age, education and gender. There are no significant differences between respondents in the two types of survey.

[Insert Table 2 about here]

3.3. Method for data analysis

Component-based partial least squares (PLS) structural equation modelling (SEM) was used to evaluate the psychometric properties of the measurement scales and to test the research hypotheses proposed in this study. PLS is widely used in information security studies (e.g. Herath & Rao, 2009b; Li, et al., 2010; Siponen & Vance, 2010; Vance & Siponen, 2012). In our study, Smart PLS software package version 2.0 was used for the estimations. We chose the variance-based PLS using Smart PLS 2.0, rather than covariance-based SEM using AMOS or LISREL, for two reasons. First, according to Haenlein and Kaplan (2004), when formative indicators are included in a model, PLS is preferable to covariance-based SEM. In our model, neutralization is a formative construct. Second, Haenlein and Kaplan (2004) noted that PLS is typically recommended in situations in which the sample size is small. The composite reliability (CR) index (Fornell & Larcker, 1981) was used to assess the reliability of the measurements. Gefen et al. (2000) suggest a CR score of at least 0.7 is required for reliable measurement. The average variance extracted (AVE) was used to assess convergent validity. An AVE value of at least 0.5 is required to establish convergent validity (Gefen, et al., 2000). The square root of the AVE and the correlations among all the constructs were used to assess the discriminant validity of the measurement. For the model estimation, the amount of variance explained (R^2) was used for assessment of the model fit.

4. Results

4.1 Descriptive statistics and the measurement model

Table 3 presents AVE, composite reliability and inter-correlations of the latent variables. The composite reliabilities for all the latent variables are greater than the 0.7 threshold, demonstrating that all constructs have adequate reliability. The AVE

values for all constructs were greater than the recommended threshold of 0.5, establishing convergent validity of the constructs. The survey instruments and item loadings are given in Table 4. The factor loadings of the measurement items on the intended constructs were at least 0.78, suggesting convergent validity. The square root of AVE for all constructs is much greater than the variance shared between the construct and other constructs, indicting good discriminant validity. Furthermore, the correlations among all constructs are well below 0.9, also suggesting discriminant validity. Intention to use the Internet for personal purposes is positively correlated with all the sub-dimensions of neutralization and perceived benefit and negatively correlated with sanction severity and detection certainty. These correlations are all in the expected direction.

[Insert Tables 3 and 4 about here]

4.2. Results of the structural model

Fig.1. shows the effect of neutralization, perceived sanction severity, perceived detection certainty and perceived benefits on intention to use the Internet for personal reasons. The model explained 65.0% of the total variance in employees' intention to use the Internet for personal purposes. Neutralization and perceived benefits were found to have a positive relationship with intention to use the Internet for personal purposes, while detection certainty was found to have a negative relationship with intention to use the Internet for personal purposes. Therefore, H1, H3, and H4 were supported. However, perceived sanction severity was found to have a non-significant relationship with intention to use the Internet for personal purposes. Therefore, H2 was not supported.

[Insert Fig.1. about here]

5. Discussion and implications

By integrating general deterrence theory and neutralization techniques, this study investigated the effect of neutralization and the perceived costs and benefits of the personal use of the Internet on intentions to use the Internet for personal reasons. The findings in this study have both theoretical and practical implications.

5.1. Main findings

As expected, we found that among all the studied variables, neutralization is the strongest predictor of intention to use the Internet for personal purposes. This finding is consistent with neutralization studies in IS security. Previous research has found that neutralization explains intention to engage in IS security policy violation (Siponen & Vance, 2010), intention to commit computer abuse (Harrington, 1996), and cyber-loafing (Lim, 2002). In addition to these quantitative research findings, some interview-based evidence from qualitative research also reported that employees try to find means to justify their deviant actions in the workplace (Lim, 2002).

Neutralization strategies are internal thought exercises that individuals employ in order to maintain a positive sense. Neutralization strategies are employed to keep the

negative emotions one feels when there is a perceived discrepancy between one's outward actions and norms of acceptable behavior in check. Neutralization techniques manifest in the form of justification and rationalization for breaking the rules in order to maintain a positive self-concept. The finding that neutralization is the strongest predictor of intention to use the Internet for personal purposes is consistent with the 'metaphor of the ledger' (Lim, 2002) and the principle of reciprocity grounded in social exchange theory (Blau, 1964). Our results are consistent with individuals either rationalizing their behavior on the basis that they are 'cashing in' on behavioral 'credits' or that they have been treated poorly by the organization in the past and reciprocal poor behavior can, thus, be justified.

The results are consistent with cognitive dissonance theory (Festinger, 1957). Cognitive dissonance theory suggests that individuals attempt to live up to internally set standards of what is morally acceptable and their positive sense of self is determined by the extent to which they are successful (Hales, 1985). When individuals engage in deviant behavior, they are able to still maintain a positive self-concept by justifying, or rationalizing away, that behavior through appropriate neutralization strategies. The results are also consistent with the theory of subjective wellbeing homeostasis (Cummins, 1998). The theory of subjective wellbeing homeostasis posits that wellbeing is managed by dispositional, genetically pre-wired, neurological systems. It posits that subjective wellbeing will lie within a set point range with an upper and lower threshold. If the set point approaches the lower threshold, there are buffers in the homeostatic mechanism that kick in to repel the challenging agent. In the context of the present study, the threat of deviant behavior to one's positive sense of self represents the challenging agent, threatening to undermine one's subjective wellbeing. Neutralization strategies, dismissing, or at least dampening, the negative consequences of one's behavior, measured in terms of one's own standards, represent a buffer, maintaining the homeostatic mechanism.

Perceived benefits were found to have a positive relationship with intention to use the Internet for personal purposes. Our finding is consistent with findings in studies by Moody and Siponen (2013) and Pee, et al. (2008) of the benefits of personal use of the Internet with Finnish and Singaporean samples respectively. The result implies that individuals who perceived that personal use of the Internet is beneficial are more likely to engage in personal use of the Internet.

The results for perceived benefits are consistent with the notion that beliefs regarding future benefits from using the Internet at work, will serve as motivation to engage in that behavior (Moody & Siponen, 2013). These potential benefits include convenience of access, social entertainment and stress relief, each of which the individual believes will result in a more rewarding work life (Li, et al., 2010; Lim & Chen, 2012; Moody & Siponen, 2013; Pee, et al., 2008).

While perceived detection certainty was found to have a negative effect on the personal use of the Internet, its effect is much smaller than the effect of neutralization or perceived benefits on the personal use of the Internet. The results for the effects of

deterrence in the IS security literature have been, at best, mixed (D'Arcy & Herath, 2011). Our results are consistent with previous studies which have found formal sanctions to have only a modest effect (Moody & Siponen, 2013) or no effect (Siponen & Vance, 2010) on Internet violation intentions. Our findings contrast with other studies in IS security research in which researchers (Cheng, et al., 2013; D'Arcy, et al., 2009; Li, et al., 2010) have reported that detection certainty and sanction severity are good predictors of intention to comply with IS security.

A possible explanation for the weaker relationship between sanction severity and intention to use the Internet for personal purposes could be that by employing neutralization techniques, people may primarily focus on justification of their behavior and, in doing so, discount, or downplay, the potential negative consequences of their actions (Hu, et al., 2011). Herath and Rao (2009a) reached the same conclusion in their study of the efficacy of certainty of apprehension and severity of punishment in a sample of US firms. They interviewed a sample of IS professionals to seek explanations for their results. One explanation offered by those interviewed by Herath and Rao (2009a) was that individuals apply a high discount rate to the penalty, such that it is considered to take effect so far into the future it is not worth being concerned about. This would be consistent with acting impulsively, while neglecting the long-term costs of one's actions. Another explanation is that individuals might feel that penalties might not really apply to them as opposed to others around them. In this respect, individuals might discount the costs of punishment because they believe that punishment is an improbable event in the future.

Our results are also consistent with findings in the economics of crime literature on the relative importance of certainty of apprehension versus severity of penalty. Becker (1968) postulated that risk neutral individuals consider only the expected penalty and not its composition, and are therefore indifferent to offsetting changes in the probability and severity of punishment that keep the expected penalty constant. Risk adverse individuals are deterred more by (equivalent) increases in severity of punishment, while risk lovers are deterred more by (equivalent) increases in the probability of detection.

Beginning with Ehrlich (1973), a consistent finding in the subsequent literature on the economics of crime is that people are deterred by the prospect of being apprehended to a much larger extent than the severity of sentence (Block & Gerety, 1995; Grogger, 1991). This result can be explained if one believes that individuals who commit crimes are preferring risk (Grogger, 1991). In our specific context, this assumes that people who engage in deviant behavior at work are prone to act impulsively, neglecting the long-term consequences of their behavior.

There is no direct empirical evidence on either the risk preference of criminals, or white collar office workers (Neilson & Winter, 1997). By the same token, it is reasonable to think that people who use the Internet at work for personal reasons, particularly when they know there is a risk of being caught and punished, are likely to prefer risk.

None the less, if one does not accept that those who engage in personal Internet use at work prefer risk in the absence of direct evidence on the point, our findings are still consistent with general deterrence theory if one steps outside the simple Becker (1968) framework. In various circumstances in which one discounts the costs of punishment or discounts the future benefits of deviant behavior, there are several scenarios in which those who engage in deviant behavior can be both risk averse and more sensitive to changes in the certainty of apprehension, than changes in the severity of punishment (Block & Lind, 1975; Mungan & Klick, 2014a, 2014b; Neilson & Winter, 1997; Polinsky & Shavell, 1999).

5.2. Theoretical contributions

The main contributions of our study to the literature on personal use of the Internet are that we examined the personal use of the Internet from a new perspective by integrating neutralization theory and general deterrence theory. In addition, we extended deterrence theory by including the benefits of personal use of the Internet. Integrating neutralization theory and deterrence theory can shed new light on understanding of behavior relating to the personal use of the Internet. Our findings demonstrated that neutralization is the largest predictor of intention to use the Internet for personal reasons. Perceived benefits of personal use of the Internet is also a good predictor. However, the effect of detection certainty on the intention to use the Internet for personal use is much weaker than the effect of neutralization and perceived benefits, while sanction severity was found to be unrelated to personal use of the Internet. These findings suggest that employees may mainly look for reasons to justify their personal use of the Internet at work. Our findings imply that given the benefits of personal use of the Internet and neutralization techniques employed to justify behavior, imposing harsher penalties will not work.

5.3. Limitations

One potential limitation of our study is related to generalizing the findings to other groups of people. Most of the respondents are young professional staff from companies in the finance and telecommunication sectors in the Northeast of China. There could be cultural differences among regions and between people of different generations. The conclusions within this paper only represent a snapshot of employees in a given region in particular industries and particularly for young professional staff that could make further generalizations outside this context problematic.

5.4. Implications for research

Our results highlight a number of opportunities for future research on personal use of the Internet. First, in our model, we incorporated five sub-dimensions of neutralization. Future research could also incorporate other sub-dimensions of neutralization such as metaphor of the ledger (Klockars, 1974). Metaphor of the ledger refers to the rationalization of individuals that they are entitled to indulge in deviant behavior because of their past good behavior (Klockars, 1974). Secondly, our research incorporated perceived detection certainty and perception of sanction

severity. Future research could incorporate other dimensions of deterrence, such as perceived celerity of sanctions (Hu, et al., 2011). Celerity represents how quickly the punishment occurs (Higgins, et al., 2005). Third, future research could also incorporate dispositions such as the Big Five personality traits in the model. Research has shown that dispositions such as the Big Five personality traits could be good predictors of personal use of the Internet (Jia, et al., 2013).

5.5. Implications for practice

Our results suggest that neutralization plays a key role in personal use of the Internet. Employers should attempt to reduce the effects of neutralization techniques. Educational sessions that emphasize the negative aspects of personal use of the Internet is one approach (Moody & Siponen, 2013). Appropriate employee training about the adverse effects of personal Internet usage at work has been shown to be an effective way to inhibit neutralization techniques (Siponen & Vance, 2010).

Perceived benefits were also found to have a significant effect on personal use of the Internet. Employers could lower perceived benefits through encouraging work-life balance and promoting more flexible working hours. This would encourage employees to browse the Internet for personal usage in non-work hours. Moody and Siponen (2013), who also found that perceived benefits is a strong predictor of Internet use, suggest that organizations need to meet employees' expectations of an interesting and rewarding work life through other avenues, such that employees do not resort to using the Internet. Their suggestion is that employees' work motivation needs to be supported by appropriate leadership approaches. This also has implications for work. It is important to recruit people who are motivated by their work.

While the certainty of apprehension was found to have a weaker effect on personal Internet use than neutralization and perceived benefits, deterrence should not be neglected. Our results suggest that increased surveillance, which will increase the probability of apprehension, will have a negative effect on intention to use the Internet in the workplace for personal reasons, although increasing the severity of the punishment will not have any effect on employee behavior.

There are several possible ways in which organizations could increase surveillance. One method would be to employ bookmark checking or informal walk-in checks to monitor the workplace (Chou, et al., 2010; Herath & Rao, 2009a). A second method would be to employ a measurement model evaluating personal webpage usage in the workplace, along the lines of that developed by Mirchandani (2004), which could be used before hiring employees (Chou, et al., 2010). A third method would be to employ one of a number of e-surveillance methods to monitor employees' usage of the Internet. E-surveillance techniques include packet sniffers, desktop monitoring, log files system administration, email filters, activity monitors and surf controllers (Sheriff & Ravishankar, 2012). While a number of commercial filtering software products exist on the market, most of these programs rely on black and white lists to block, or allow, Internet access. This creates several problems (Chou,

et al., 2010). One problem is that for organizations, maintaining the lists is very expensive. Another problem is that while commercial filter providers typically periodically update the lists, they still might be out of date. Hunter (2000) found that four popular commercial filters (CYBERsitter, CyberPatrol, Net Nanny and Surf Watch) exhibited Over-inclusive and Under-inclusive blocking error rates due to source-based filtering, which relies on pre-defined black and white lists. For this reason, text mining approaches represent a better alternative to commercial filters based on maintaining lists, as a method to monitor employees (Chou, et al., 2010).

6. Conclusion

This study has contributed to the extant literature on the understanding of personal use of the Internet drawing on neutralization and general deterrence theories. The findings from this study support the tenets of neutralization theory that employees will use various neutralization techniques to justify their deviant behavior in the workplace. In our study, the deviant behavior represents personal use of the Internet. In addition, we found that perceived benefits have an influence on personal use of the Internet. Although detection certainty was also found to have an effect on intention to use the Internet for personal reasons, its effect was much weaker than those of neutralization and perception of benefits. The results imply that employees concentrate on the perceived benefits of personal Internet use while, at the same time, finding justification for their behavior and paying less attention to the expected punishment. To the extent that individuals do turn their mind to the implications of being caught, they are more concerned with the probability of being caught than the severity of the punishment once caught, which has an insignificant effect on behavior. This latter result is consistent with employees who express an intention to use the Internet for personal reasons at work, when such behavior is not permitted, being risk lovers.

Acknowledgements

This work is partially supported by the National Natural Science Foundation of China under Grant No. 71272092. We thank the editor and the reviewers for their comments and suggestions.

References

Becker, G. (1968). Crime and punishment: An economic approach. *Journal of Political Economy,* 76, 169-217.

Blanchard, A.L., & Henle, C.A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior,* 24(3), 1067-1084.

Blau, P.M. (1964). *Exchange and power in social life*. New York: Wiley.

Block, M.K., & Gerety, V.E. (1995). Some experimental evidence on differences between student and prisoner reactions to monetary penalties and risk. *The Journal of Legal Studies*, 123-138.

Block, M.K., & Lind, R.C. (1975). An economic analysis of crimes punishable by imprisonment. *Journal of Legal Studies,* 4, 479-492.

Bock, G.W., & Ho, S.L. (2009). Non-work related computing (NWRC). *Communications of the ACM,* 52(4), 124-128.

Brislin, R.W. (1993). *Understanding culture's influence on behavior*. Fort Worth: Harcourt Brace Jovanovich College Publishers.

Buzzell, T. (2005). Holiday revelry and legal control of fireworks: A study of neutralization in two normative contexts. *Western Criminology Review,* 6(1), 30-42.

Case, C.J., & Young, K.S. (2002). Employee Internet management: Current business practices and outcomes. *CyberPsychology & Behavior,* 5(4), 355-361.

Chen, J.V., Ross, W.H., & Yang, H.-H. (2011). Personality and motivational factors predicting Internet abuse at work. *Journal of Psychosocial Research on Cyberspace,* 5, 1-12.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security,* 39, 447-459.

Chou, C., Sinha, A.P., & Zhao, H. (2010). Commercial Internet filters: Perils and opportunities. *Decision Support Systems,* 48(4), 521-530.

Cook, C., Heath, F., & Thompson, R.L. (2000). A meta-analysis of response rates in web-or Internet-based surveys. *Educational and Psychological Measurement,* 60(6), 821-836.

Cummins, R.A. (1998). The second approximation to an international standard for life satisfaction. *Social Indicators Research,* 43(3), 307-334.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems,* 20(6), 643-658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research,* 20(1), 79-98.

Ehrlich, I. (1973). Participation in illegitimate activities: A theoretical and empirical investigation. *Journal of Political Economy,* 81(3), 521-565.

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford: Stanford University Press.

Fornell, C., & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39-50.

Garrett, R.K., & Danziger, J.N. (2008a). Disaffection or expected outcomes: Understanding personal Internet use during work. *Journal of Computer‐Mediated Communication,* 13(4), 937-958.

Garrett, R.K., & Danziger, J.N. (2008b). On cyberslacking: Workplace status and personal Internet use at work. *CyberPsychology & Behavior,* 11(3), 287-292.

Gefen, D., D.W.Straub, & Boudreau, M.C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the AIS,* 4, 1-77.

Grogger, J. (1991). Certainty vs. severity of punishment. *Economic Inquiry,* 29(2), 297-309.

Haenlein, M., & Kaplan, A.M. (2004). A beginner's guide to partial least squares analysis. *Understanding Statistics,* 3(4), 283–297.

Hales, S. (1985). The inadvertent rediscovery of self in social psychology. *Journal for the Theory of Social Behaviour,* 15, 237-282.

Harrington, S.J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS Quarterly,* 20(3), 257-278.

Harris, L.C., & Dumas, A. (2009). Online consumer misbehaviour: An application of neutralization theory. *Marketing Theory,* 9(4), 379-402.

Herath, T., & Rao, H.R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems,* 47(2), 154-165.

Herath, T., & Rao, H.R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems,* 18(2), 106-125.

Higgins, G.E., Wilson, A.L., & Fell, B.D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture,* 12(3), 166-184.

Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology,* 9(3), 187-204.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM,* 54(6), 54-60.

Hunter, C.D. (2000). Social impacts Internet filter effectiveness: Testing over and underinclusive blocking decisions of four popular web filters. *Social Science Computer Review,* 18(2), 214-222.

Jarvis, C.B., Mackenzie, S., Podsakoff, P., Mick, D., & Bearden, W. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journals of Consumer Research,* 30(2), 199-218.

Jia, H., Jia, R., & Karau, S. (2013). Cyberloafing and personality: The impact of the big five traits and workplace situational factors. *Journal of Leadership & Organizational Studies,* 20(3), 358-365.

Johnson, P.R., & Indvik, J. (2004). The organizational benefits of reducing cyberslacking in the workplace. *Journal of Organizational Culture, Communications, and Conflict,* 8, 55–62.

Kankanhalli, A., Teo, H.-H., Tan, B.C.Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management,* 23(2), 139-154.

Kim, S.J., & Byrne, S. (2011). Conceptualizing personal web usage in work contexts: A preliminary framework. *Computers in Human Behavior,* 27, 2271-2283.

Klockars, C.B. (1974). *The professional fence*. New York: Macmillan.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with Internet use policy from the perspective of rational choice theory. *Decision Support Systems,* 48(4), 635-645.

Lim, V.K.G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior,* 23(5), 675-694.

Lim, V.K.G., & Chen, D.J.Q. (2012). Cyberloafing at the workplace: Gain or drain on work? *Behaviour & Information Technology,* 31(4), 343-353.

McBride, M., Carter, L., & Warkentin, M. (2012). One size doesn't fit all: Cybersecurity training should be customized. In: *Technical report, Institute for Homeland Security Solutions, 2012.* http://sites.duke.edu/ihss/files/2011/12/CyberSecurity_2page-summary_mcbride-2012.pdf.

Mirchandani, D., & Motwani, J. (2003). Reducing Internet abuse in the workplace. *SAM Advanced Management Journal,* 68(1), 22-26.

Mirchandani, D.A. (2004). A deterrence theory perspective on personal web usage in personal web usage in workplace: A guide to effective human resources management. In *C.A. Simmers (ed.), Information Science Publisher, Hershey, PA* (pp. 111-124).

Moody, G.D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information & Management,* 50, 322-335.

Morris, R.G., & Higgins, G.E. (2009). Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review,* 34(2), 173-195.

Mungan, M.C., & Klick, J. (2014a). Discounting and criminals' implied risk preferences. *SSRN Working Paper* http://ssrn.com/abstract=2396892.

Mungan, M.C., & Klick, J. (2014b). Forfeiture of illegal gains, attempts and implied risk preferences. *Journal of Legal Studies, Forthcoming*.

Neilson, W.S., & Winter, H. (1997). On criminals' risk attitudes. *Economics Letters,* 55(1), 97-102.

Pee, L.G., Woon, I.M.Y., & Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information & Management,* 45(2), 120-130.

Polinsky, A.M., & Shavell, S. (1999). On the disutility and discounting of imprisonment and the theory of deterrence. *Journal of Legal Studies,* 28, 1-16.

Posey, C., Bennett, B., Roberts, T., & Lowry, P. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security,* 7(1), 24-47.

Rajah, R., & Lim, V.K.G. (2011). Cyberloafing, neutralization and organizational citizenship behavior. In *Pacific Asia Conference on Information Systems, PACIS2011*.

Sheriff, A.M., & Ravishankar, G. (2012). The techniques and rationale of E-surveillance practices in organizations. *International Journal of Multidisciplinary Research,* 2(2), 281-290.

Siau, K., Nah, F.F.H., & Teng, L. (2002). Acceptable Internet use policy. *Communications of the ACM,* 45(1), 75-79.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly,* 34(3), 487-502.

Sykes, G.M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review,* 22(6), 664-670.

Ugrin, J., & Pearson, J.M. (2008). Exploring Internet abuse in the workplace: How can we maximize deterrence efforts? *Review of Business Journal,* 28(2), 29-40.

Ugrin, J.C., & Pearson, J.M. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior,* 29(3), 812-820.

Vance, A., & Siponen, M.T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC),* 24(1), 21-41.

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior,* 27, 1751–1759.

Wenzel, M. (2004). The social side of sanctions: Personal and social norms as moderators of deterrence. *Law and Human Behavior,* 28(5), 547-567.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly,* 37(1), 1-20.

Young, K. (2010). Killer surf issues: Crafting an organizational model to combat employee Internet abuse. *Information Management Journal,* 44(1), 34-38.

Young, K. (2011). Internet abuse in the workplace. *Academy of Business Research Journal,* 2, 20-29.

Young, K.S., & Case, C.J. (2004). Internet abuse in the workplace: New trends in risk management. *CyberPsychology & Behavior,* 7(1), 105-111.

Table 1

Profile of respondents.

Variables	N	%
Gender		
Male	143	62.2
Female	87	37.8
Age		
18 to 24	44	19.1
25 to 34	165	71.7
35 and over	21	9.1
Education		
Polytechnic and below	52	22.6
Bachelor	110	47.8
Master and PhD	68	29.6
Working years		
Less than 3 years	175	76.1
3 to 5 years	25	10.9
More than 5 years	30	13.0
Computer usage per day		
Less than 4 hours	33	14.3
4 to 6 hours	41	17.8
More than 6 hours	156	67.8

Table 2

Profile of respondents to the online and paper surveys.

		Online survey		Paper survey	
		No.	%	No.	%
Gender	Male	68	60.7%	75	63.6%
	Female	44	39.3%	43	36.4%
Age	18 to 24	22	19.6%	22	18.6%
	25 to 34	80	71.4%	85	72.0%
	35 and over	10	8.9%	11	9.3%
Education	Polytechnic and below	30	26.8%	22	18.6%
	Bachelor	48	42.9%	62	52.5%
	Master and PhD	34	30.4%	34	28.8%

Table 3

AVE, composite reliability and inter-correlations of the latent variables.

	AVE	CR	1	2	3	4	5	6	7	8	9
1.DenRes	**0.83**	**0.89**	**0.91**								
2.DenInj	**0.70**	**0.79**	0.50	**0.84**							
3.DenVic	**0.73**	**0.81**	0.45	0.54	**0.85**						
4.ConCon	**0.77**	**0.85**	0.46	0.43	0.51	**0.88**					
5.AppHLoy	**0.78**	**0.86**	0.51	0.46	0.42	0.54	**0.89**				
6.SanSev	**0.85**	**0.91**	-0.20	-0.25	-0.20	-0.19	-0.08	**0.92**			
7.DetCer	**0.90**	**0.89**	-0.53	-0.49	-0.47	-0.49	-0.50	0.33	**0.95**		
8.PerBen	**0.71**	**0.86**	0.53	0.45	0.41	0.42	0.45	-0.17	-0.50	**0.84**	
9.Int	**0.78**	**0.86**	0.56	0.58	0.61	0.56	0.57	-0.18	-0.59	0.62	**0.88**

Notes: DenRes = denial of responsibility; DenInj = denial of injury; DenVic = denial of victim; ConCon = condemnation of the condemners; AppHloy= appeal to higher loyalties; SanSev = sanction severity; DetCer = detection certainty; PerBen = perceived benefits; Int = intention to use the Internet for personal reasons. . The bold values on the diagonal show the square roots of AVEs. For $r > 0.18$, correlation is significant at the 0.01 level (2-tailed); for $r < 0.18$ and $r > 0.14$, correlation is significant at the 0.05 level.

Table 4

Measurement items and item factor loading.

Constructs	Items	Source	Loading
Int	I intend to use the Internet provided by the organization for non-work-related purposes in the future.	Adapted from Pee et al. (2008)	0.900
	I will use the Internet provided by the organization for non-work-related purposes in the future.		0.908
	I expect to use the Internet provided by the organization for non-work-related purposes in the future.		0.822
DetCer	If I used the Internet access provided by the organization for non-work-related purposes, the probability that I would be caught is (Very Low/Very High).	Adapted from Li et al. (2010)	0.933
	I would probably be caught (Very Low/Very High).		0.948
SanSev	If I was caught using the Internet access provided by the organization for non-work-related purposes, I think the punishment would be (Very Low/Very High).	Adapted from Li et al. (2010)	0.877
	I would be severely punished by my organization.		0.919
	My Internet access privileges would be restricted by the organization.		0.938
PerBen	Using the Internet access provided by the organization for non-work-related purpose will allow me to spend less private (non-work) time accessing the Internet.	Adapted from Li et al. (2010)	0.823
	Reduce my personal expense of accessing the Internet.		0.821
	Convenience.		0.800
	More interesting work life.		0.825
DenRes	It is OK to use the Internet access provided by the organization for personal purposes if I am not sure whether there is Internet use policy in the organization.	Adapted from Siponen and Vance (2010)	0.901
	It is OK to use the Internet access provided by the organization for personal purpose if the Internet use policy is not explicitly advertised.		0.911
	It is OK to use the Internet access provided by the organization for personal purposes if I don't understand the Internet use policy.		0.898
DenInj	It is OK to use the Internet access provided by the organization for personal purposes if no harm is done.	Adapted from Siponen and Vance (2010)	0.840
	It is OK to use the Internet access provided by the organization for personal purposes if no damage is done to the company.		0.851
	It is OK to use the Internet access provided by the		0.833

	organization for personal purposes if no one gets hurt.		
DenVic	If the managers are worried about harm from personal use of the Internet they should have better online management.	Adapted from Morris & Higgins(2009)	0.874
	I don't really buy into the idea that the company loses much from personal use of the Internet.		0.884
	It is OK to surf the net for non-work reasons because my boss is biased and does not treat us well.		0.781
ConCon	Managers should be more worried about other kinds of misconduct than personal use of the Internet.	Adapted from Buzzell(2005)	0.865
	The Company where I work really should worry about other issues than personal use of the Internet.		0.891
	The Company has been ripping its employees off for years, so personal use of the Internet is justified.		0.880
AppHloy	It is OK to use the Internet access provided by the organization for personal purposes if it is somehow used to benefit an individual or a business.	Adapted from Hinduja (2007)	0.881
	It is all right to use the Internet access provided by the organization for personal purposes to get my work done more efficiently.		0.902
	It is OK to use the Internet access provided by the organization for personal purposes if a family member, friend, or significant other needs me to do so.		0.887

Notes: DenRes = denial of responsibility; DenInj = denial of injury; DenVic = denial of victim; ConCon = condemnation of the condemners; AppHloy= appeal to higher loyalties; SanSev = sanction severity; DetCer = detection certainty; PerBen = perceived benefits; Int = intention to use the Internet for personal reasons.