Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2013 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-18-2013

Effects of Neutralization Techniques and Rational Choice Theory on Internet Abuse in the Workplace

Wenli Li
Dalian University of Technology, wlli@dlut.edu.cn

Lijiao Cheng
Dalian University of Technology, imchenglijiao@gmail.com

EFFECTS OF NEUTRALIZATION TECHNIQUES AND RATIONAL CHOICE THEORY ON INTERNET ABUSE IN THE WORKPLACE

Wenli Li, Faculty of Management and Economics, Dalian University of Technology, Dalian, Liaoning, P.R.China, wlli@dlut.edu.cn

Lijiao Cheng, Faculty of Management and Economics, Dalian University of Technology, Dalian, Liaoning, P.R.China, imchenglijiao@gmail.com

Abstract

This research aims to identify the antecedents that drive an employee to commit Internet abuses at the workplace. Drawing on literatures in criminology, this present study developed a theoretical model based on neutralization techniques and rational choice theory. The model was validated using survey data from 428 employees. Our results indicate that neutralization techniques significantly influence employees' Internet abuse intentions except denial of responsibility. The cost-benefits analysis of perceived security risks and perceived benefits are also found to play an important role in affecting Internet abuse intentions while the risks of perceived formal sanctions have no significant effect. We then discuss key implications of our findings for research and practice.

Keywords: Workplace deviant, Internet Abuse, Neutralization Techniques, Rational Choice Theory.

1 INTRODUCTION

The Internet has become more critical in changing the way organizations do business and empowering employees to perform their tasks (Vitak, et al., 2011). However, access to websites through the Internet may be easily abused by employees. Internet abuse, also referred to as non-work-related computing(NWRC), cyberloafing, cyberslacking, cyber deviance, personal use at work, and junk computing, is employees' usage of the organizational Internet access during work hours for non-work-related purposes(Young, 1996). There is no consensus definition of this broad phenomenon. In our research, Internet abuse behaviours include but not limited to Internet browsing (i.e. reading news on the Internet), downloading files for personal purposes (i.e. movies and music), personal e-commerce (i.e. online shopping, tracking stock prices), personal communication (i.e. online chatting by QQ, MSN), or even getting involved in cybercrimes (Bock & Ho, 2009; Lee, et al., 2004). According to recent studies, human resource professionals assumed that employees waste around 1 hour engaging in personal purpose activities using the Internet (Bloxx, 2008, Rajah R. &Lim V.K.G.,2011); While employees have admitted to wasting approximately two hours each day (Lim & Chen, 2012; Vitak, et al., 2011). An International Data Corporation (IDC) survey indicates that 30 to 40 per cent of on-the-job Internet use is non business related (Spy., 2011). These non-work-related Internet activities not only lead to financial losses from reduced productivity of employees but also can cause other problems such as reduced bandwidth and legal issues, along with security concerns (Case & Young, 2002; Lim, 2002; Lim, et al., 2002). It is of vital importance for enterprises to curb Internet abuses and regulate the usage of Internet.

To cope with the epidemic of Internet abuse, companies set up Internet usage policy and control mechanisms to reduce these activities (Case & Young, 2002; Kankanhalli, et al., 2003; Mirchandani & Motwani, 2003; Mirchandani, 2004). However, contrary to what might be expected, Internet abuse is still an issue in the workplace (Bock & Ho, 2009; Lee, et al., 2008; Lim & Chen, 2012; Pee, et al., 2008; Young & Case, 2004). Lee, et al. (2004) have stated that monitoring, enforcement and punishment mechanisms only emphasize sanctions and technology uses but ignores human concerns. From the perspective of compensatory behaviours, we proposed that individuals engage in either neutralization techniques or rational choice theory as compensation for Internet abuse at work. Our results show that all neutralization techniques (except denial of responsibility) and perceived security risks, perceived benefits significantly influence employees' Internet abuse intentions. The findings have implications for Internet usage practice and research. Our results also suggest that practitioners should especially make effort to counteract employees' use of neutralization techniques.

The remainder of the paper is structured as follows. The next section presents a brief review of previous relevant literatures, followed by our theoretical research model and the hypotheses to be tested. Next, we describe a summary of the research method and the results. We then discussed the results, limitations, and implications for future research and practice. Finally, we conclude with our major findings.

2 LITERATURE REVIEW

Recent research has shown, however, that accessing the Internet for non-work-related activities can serve as a perquisite – a way that awakening creativity, which also allows employees to recover from the job stress and helps to refresh and revitalize employees' minds (Lim & Chen, 2012). It was much the same as making personal calls or chatting at the water cooler (Wong et al. 2005). Yet, when employees abuse the Internet at work, such as receiving non-work-related emails, they are essentially juggling multiple mental tasks at the same time. Greenfield (2009) found that individuals performed worse in the tasks assigned when engaged in multi-tasking. Bock & Ho (2009) also found that non-work-related computing truly reduce employees productivity. That's why Internet abuse has been seen as a form of work deviant and managers in the enterprise should pay attention to.

Previous researches related to Internet abuse is mainly descriptive (Al-Saad & Saleh, 2011; Lim & Teo, 2005; Lim, et al., 2002; Young, 2010; Young & Case, 2004). Although description is a vital first

step when researching a new construct, in attempting to understand the personal and organizational factors affecting employees' Internet abuse behaviours, little previous work has applied several theoretical perspectives, mainly including general deterrence theory (Henle & Blanchard, 2008; Kankanhalli, et al., 2003; Mahatanankoon, et al., 2004; Mirchandani, 2004; Ugrin & Pearson, 2007; Velezmoro, et al., 2010; Woon & Pee, 2004), Theory of interpersonal behaviour(Lee, et al., 2005; Pee, et al., 2008), and neutralization(Rajah & Lim, 2011). Ugrin and Pearson (2007) indicated that a series of well-defined Internet acceptable use policies, potential sanctions, and detection (or monitoring) performance mechanisms is an important deterrent of Internet abuse. Garrett and Danziger (2008) found that occupational status, job autonomy within the workplace, income, education, and gender were significant antecedents of cyberslacking. They concluded that high-status employees were more frequently engaged in personal Internet use at work. Lee, et al. (2005) revealed that IS environmental factor and habit were strong predictors of NWRC behaviour. Pee, et al. (2008) also found that affect, social factors, and perceived consequences were significant predictors of employees' NWRC engagement intention, while intention to engage in it, habit, and facilitating conditions significantly influenced employees' NWRC behaviour. Bock, et al. (2007) integrated Internet abuse control measures with task characteristics and organizational culture. The results suggested that under high degree of task non-routineness, the control mechanisms became ineffectiveness. Furthermore, the more fitness between discipline systems and organization culture, the higher employee satisfaction with NWRC management, which subsequently led to lower NWRC engagement. What's more, there is no best Internet use rule for each organization. Rajah and Lim (2011) found that individuals tended to engage in neutralization or organizational citizenship behaviour compensation techniques to justify their cyberloafing at work. The current study seeks to expand on previous studies by examining two of the leading criminological explanations of deviant behaviours, namely neutralization techniques and rational choice theory, to Internet abuse in the workplace.

3 RESEARCH MODEL AND HYPOTHESES

In the following section we preface the theoretical model for the research and hypothesize the relationships between constructs. Our model comprises two theories from the field of Criminology: neutralization theory(Sykes & Matza, 1957) and rational choice theory (von Neumann & Morgenstern, 1944).

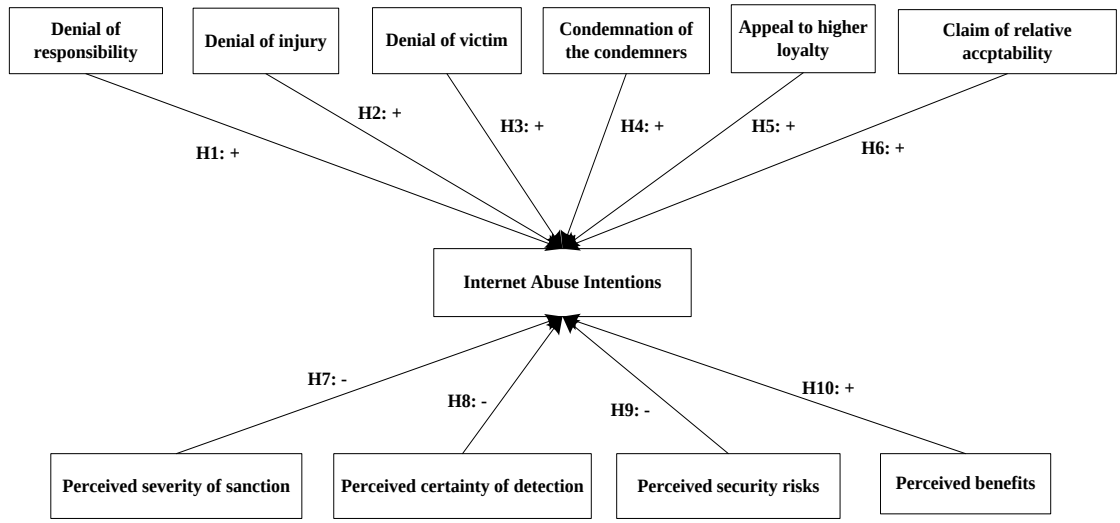

Figure 1. Research model

3.1 Neutralization techniques

Neutralization Theory was introduced in an attempt to demonstrate how juveniles are able to escape from normative societal restrictions so that rule-breaking or any anti-social actions can be committed (Sykes & Matza, 1957). And lately, organizational scholars are beginning to take the appeal of

neutralization techniques into account as a better explanatory to understand workplace deviance. Neutralization techniques offer persons a way to shrug off existing norms ineffective by justifying actions that runs counter to those norms (Rogers & Buffalo, 1974). In the context of this study, we adopt the first five techniques of neutralization proposed in Sykes and Matza's seminal piece: denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, and appeal to higher loyalties; as well as one another rationalization: claim of relative acceptability (Henry, 1990). Denial of responsibility places the blame on alternative source or circumstance which compelled or coerced the misbehaviour. In other words, the responsibility is shifted to someone else other than the self. They are not really guilty due to 'factors beyond their control' caused their deviant activity (Harris & Dumas, 2009). In using of denial of injury, the individual may conclude that no harm to organizational property or to other individuals will result from Internet abuse, thus participation in the behaviour is lack of direct harm and thus making the behaviour more acceptable. Denial of victim might be used when the victim is not physically visible or is unknown or abstract. A different view of this technique acknowledges that the violated party deserved whatever happened. Condemnation of the condemners refers an expression of discontent with the perceptions of the 'condemners'. By criticizing the behaviour of authority holders, the delinquent is able to shift the focus of attention away from his/her own actions to those who criticize them. Appeal to higher loyalties refers to justifying their aberrant behaviours as being parts of a higher order ideal or value equal to or greater than one's own self-interest. Claim of relative acceptability avoids culpability by drawing a comparison with more reprehensible deeds to minimize the consequences of the deviant behaviour.

These techniques of neutralization have widely utilized by individuals to excuse a deviant act or behaviour by providing acceptable justifications. Siponen, et al. (2012) studied the effects of neutralization techniques on software piracy intentions. And results showed that two of the neutralization techniques, appeal to higher loyalties and condemnation of the condemners, strongly predicted software piracy intentions. In another piece of paper, Siponen and Vance (2010) showed that neutralization theory offered a new insight of explanations for IS security policy violations. Lim (2002) used an extension neutralization technique, the metaphor of the ledger, to explain how individuals rationalize their deviant behaviours by viewing such actions as acceptable in their minds. As mentioned before, research has identified that many offenders do not take Internet abuses in a negative light. Employees tend to justify their counterproductive work behaviour by neutralization techniques. Thus we can hypothesize:

H1. Denial of responsibility will positively affect employees' intention to Internet abuse.

H2. Denial of injury will positively affect employees' intention to Internet abuse.

H3. Denial of victim will positively affect employees' intention to Internet abuse.

H4. Condemnation of the condemners will positively affect employees' intention to Internet abuse.

H5. Appeal to higher loyalties will positively affect employees' intention to Internet abuse.

H6. Claim of relative acceptability will positively affect employees' intention to Internet abuse.

3.2 Rational Choice variables

Rational choice theory is a neo-classical economic measure offering a theoretical explanation for how individuals make decisions when faced with choices (Bulgurcu, et al., 2010). The theory suggests that cost–benefit analyses of an individual's options determine how he will act. Employees are apt to abuse the Internet when perceived benefits of Internet abuse exceed the potential risks from sanctions and security threats. Potential risks of Internet abuse include the possibility and severity of sanctions and security risks that Internet abuse can expose the organizational computer and information to. Perceived benefits of Internet abuse could be the time and money saved over using private Internet access at other place, convenience, or emotional benefits such as making the work life more funny and interesting (Li, et al., 2010).

3.2.1 Sanctions

Rational choice theory has affirmed sanctions as important instruments for deterring aberrant behaviours (Paternoster & Simpson, 1996). In this study, we include two deterrence mechanisms dimensions: perceived severity of sanction and perceived certainty of detection. Severity means that an individual believes that his or her criminal behaviour will be harshly punished while certainty means the probability that they will be caught. They are both a form of perceived risk to commit Internet abuse. D'Arcy, et al. (2009) developed an extended deterrence model that predicted that perceived certainty and severity of organizational sanctions influence individuals' IS misuse intention. In our research context, Internet abuse will be more likely to be used as a coping strategy when employees perceive there are few, if any, sanctions for doing so. Hence,

H7. Perceived severity of sanction will negatively affect employees' intention to Internet abuse.

H8. Perceived certainty of detection will negatively affect employees' intention to Internet abuse.

3.2.2 Perceived security risks

Perceived security risks are the degree of perceived Internet security risks in the workplace. In modern technology era, the Internet has been regarded as the vital platform for virus attacks. Abusing Internet access in the workplace increases the chance of organizational computer or data exposure to Internet security breaches. So, perceived security risks may act as another fear-based mechanism that increases the cost of Internet abuses. In general, when individuals perceive a threat, they often adjust their behaviours in response to the amount of risk and determine if they are willing to accept the threat or not (Li, et al., 2010; Woon, et al., 2005). Thus, an individual's perceived security risks tend to be negatively linked to their intentions to Internet abuses. Therefore,

H9. Perceived security risks will negatively affect employees intention to Internet abuse.

3.2.3 Perceived benefits

According to rational choice theory, potential offenders take a cost/benefit trade-off before committing any deviant behaviour. We define perceived benefits as the overall expected favourable consequences an employee could get from Internet abuses. It can be the time or money saved by using private Internet access. Convenience was perceived to be another significant benefit of Internet abuse. In addition, some employees also use the Internet for entertainment purposes such as downloading movies and gaming (Johnson & Indvik, 2004; Pee, et al., 2008). These perceived benefits of Internet abuse may override the impact of sanctions and security threats, and lead to Internet abuses. Therefore,

H10. Perceived benefits will positively affect employees intention to Internet abuse.

4 METHOD

4.1 Measurement items

To validate measurement instruments for the proposed theoretical model, a questionnaire-based field survey was conducted with organizational employees to collect data. The process of item development began with an investigation of previous theoretical and empirical literature. Items were drawn from previously validated instruments where possible. The final questionnaire includes two sections. The first section collects basic information related to responders and organizations. The second section contains neutralization techniques and risk-benefits analysis questions. All constructs were measured reflectively with multiple items on seven-point Likert scales.

For the pilot study, the survey questionnaires were distributed to 50 midlevel managers at five local companies in China. Both Measurement items reliabilities and discriminant validity assessments yielded acceptable results in almost all samples. On the basis of the pilot study results, we did a few

revisions of the wording clarifying, order of items, and format of the questionnaire. And a new questionnaire was developed.

4.2 Data collection

We then collected primary data from two ways. On one hand, we sent 500 paper editions questionnaires to employees in 15 local organizations and 253 completed the survey. On the other hand, we designed an online survey in a professional survey website. We send emails to invite some employees in other cities to complete the online survey. There are 620 people received our invitation, 206 completed the survey. Of the remaining 459 respondents, 31 were later discarded because of incomplete answers or indicated unreliable (i.e., answers exhibiting certain unlikely patterns, such as all 4 or alternating 3 and 4). Hence, 428 usable sample questionnaires were included in this analysis, giving an effective response rate of 38%. In the final sample, 54% of the respondents were male, 45% have a degree of bachelor, and 74% were in the 25-34 age range. The average usage of the computer per day was 7-10 hours. 25% of the respondents reported working for telecom/computer companies. As for Internet usage policies, 46% of the respondents reported there is no clear announcement in their organization, while 26% reported having the Internet usage policies for more than 5 years.

Category		Percent	Category		Percent
Gender	Male	53.8%	Working years	<3 year	72.9%
	Female	46.2%		3~5 years	12.1%
Age	18~24	18.3%		>5 years	15%
	25~34	74.2%	Computer usage	< 4 hours	10.5%
	35 and over	7.5%	(hrs./day)	4~6 hours	19.4%
Education	Below bachelor	31.2%		>6 hours	70.1%
	Bachelor	45.2%	Internet usage policy	No	46.2%
	Master	23.6%		Yes	53.8%

Table 1. Demographic characteristics.

5 DATA ANALYSES AND RESULTS

The research models and hypotheses were assessed by partial least squares (PLS), a structural equation modelling (SEM) tool. PLS was chosen for two reasons. First, it can concurrently test both the measurement model and the structural model. Second, it has less stringent distribution assumptions. Specifically, SmartPLS was used in our data estimations.

5.1 Measurement model

The measurement model assessment involves the evaluation of construct reliability, convergent validity, and discriminant validity of the instrument items. Construct reliability is the degree to which items are free from random error, and generate similar scores. Convergent validity measures the degree to which the multi-items measuring the same construct agree (Cook & Campbell, 1979). While discriminant validity is the degree to which a construct is differentiate from other constructs.

The measure of construct reliability was assessed using the composite reliability (CR) index. As shown in Table 2, the composite reliabilities for all constructs are greater than the 0.70 threshold, demonstrating that all constructs have adequate reliability (Gefen, et al., 2000).

	AVE	CR	1	2	3	4	5	6	7	8	9	10	11
1.INT	0.78	0.92	**0.88**										
2.DenRes	0.83	0.93	0.56	**0.91**									
3.DenInj	0.70	0.88	0.59	0.50	**0.84**								
4.DenVic	0.73	0.89	0.61	0.46	0.54	**0.85**							
5.ConCon	0.77	0.91	0.56	0.46	0.43	0.51	**0.88**						
6.AppHLoy	0.78	0.92	0.57	0.51	0.46	0.42	0.54	**0.89**					
7.ClReAcc	0.82	0.93	0.56	0.42	0.42	0.44	0.39	0.40	**0.90**				
8.SanSev	0.85	0.94	-0.18	-0.20	-0.25	-0.20	-0.19	-0.08	-0.11	**0.92**			
9.DetCer	0.90	0.95	-0.59	-0.53	-0.49	-0.47	-0.48	-0.50	-0.44	0.33	**0.95**		
10.PerSec	0.72	0.91	-0.61	-0.40	-0.45	-0.43	-0.38	-0.41	-0.42	0.32	0.67	**0.85**	
11.PerBen	0.71	0.91	0.62	0.53	0.45	0.41	0.42	0.45	0.45	-0.17	-0.50	-0.38	**0.84**

Table 2. Reliability and Correlation of the Latent Variable Scores

Convergent and discriminant validity were assessed using composite reliability of each scale, and average variance extracted (AVE) for each construct, factor analysis and item correlations. The AVE values for all constructs were greater than the recommended threshold value of 0.50 (Convergent Validity). The square root of AVE for each construct (the principal diagonal element) is much greater than the variance shared between the construct and other constructs (Discriminant Validity). All standardized item loadings on respective constructs were at least 0.70 (Convergent Validity) (Chin & Marcolin, 1995). All the factor loadings of measurement items on their intended constructs were above 0.78 and at least an order of magnitude larger than cross-loadings (Discriminant Validity) (Gefen, et al., 2000). Thus, we concluded that the convergent and discriminant validity of all scales were adequate.

	1	2	3	4	5	6	7	8	9	10	11
DenRes1	**0.91**	0.44	0.42	0.45	0.47	0.40	-0.14	-0.48	-0.36	0.47	0.51
DenRes2	**0.91**	0.45	0.40	0.40	0.46	0.37	-0.20	-0.49	-0.38	0.49	0.50
DenRes3	**0.91**	0.47	0.42	0.42	0.45	0.38	-0.19	-0.47	-0.37	0.48	0.53
DenInj1	0.41	**0.82**	0.44	0.39	0.41	0.27	-0.24	-0.45	-0.41	0.38	0.49
DenInj2	0.47	**0.84**	0.46	0.40	0.42	0.41	-0.21	-0.45	-0.35	0.36	0.47
DenInj3	0.37	**0.85**	0.46	0.29	0.32	0.38	-0.19	-0.33	-0.38	0.39	0.51
DenVic1	0.40	0.48	**0.88**	0.47	0.37	0.36	-0.17	-0.40	-0.38	0.37	0.53
DenVic2	0.43	0.46	**0.89**	0.46	0.38	0.34	-0.17	-0.42	-0.37	0.37	0.54
DenVic3	0.33	0.44	**0.78**	0.37	0.31	0.43	-0.17	-0.37	-0.36	0.33	0.48
ConCon1	0.39	0.37	0.45	**0.87**	0.46	0.36	-0.19	-0.44	-0.34	0.37	0.46
ConCon2	0.44	0.36	0.46	**0.88**	0.50	0.31	-0.13	-0.44	-0.32	0.39	0.49
ConCon3	0.40	0.40	0.45	**0.89**	0.46	0.37	-0.20	-0.40	-0.34	0.36	0.53
AppHLoy1	0.44	0.43	0.38	0.43	**0.88**	0.36	-0.09	-0.43	-0.36	0.38	0.50
AppHLoy2	0.45	0.42	0.39	0.51	**0.90**	0.38	-0.09	-0.46	-0.39	0.43	0.54
AppHLoy3	0.47	0.37	0.35	0.48	**0.87**	0.32	-0.04	-0.44	-0.34	0.39	0.48
ClReAcc1	0.35	0.36	0.37	0.33	0.34	**0.89**	-0.10	-0.36	-0.35	0.40	0.48
ClReAcc2	0.41	0.40	0.40	0.37	0.37	**0.91**	-0.12	-0.40	-0.38	0.40	0.52
ClReAcc3	0.38	0.38	0.42	0.37	0.37	**0.91**	-0.08	-0.42	-0.41	0.43	0.51
SanSev1	-0.19	-0.23	-0.18	-0.20	-0.08	-0.09	**0.92**	0.29	0.28	-0.14	-0.16
SanSev2	-0.18	-0.23	-0.19	-0.18	-0.08	-0.11	**0.93**	0.30	0.30	-0.15	-0.18
SanSev3	-0.17	-0.24	-0.18	-0.16	-0.07	-0.10	**0.91**	0.30	0.30	-0.16	-0.17
DetCer1	-0.51	-0.45	-0.43	-0.46	-0.44	-0.41	0.32	**0.95**	0.63	-0.47	-0.55

DetCer2	-0.50	-0.48	-0.46	-0.46	-0.51	-0.42	0.30	**0.95**	0.64	-0.48	-0.58
PerSec1	-0.38	-0.41	-0.36	-0.32	-0.29	-0.45	0.36	0.58	**0.78**	-0.37	-0.47
PerSec2	-0.35	-0.43	-0.42	-0.35	-0.40	-0.36	0.22	0.54	**0.88**	-0.34	-0.55
PerSec3	-0.37	-0.34	-0.35	-0.36	-0.39	-0.31	0.24	0.59	**0.86**	-0.29	-0.51
PerSec4	-0.28	-0.36	-0.34	-0.29	-0.31	-0.33	0.29	0.56	**0.88**	-0.31	-0.53
PerBen1	0.50	0.37	0.35	0.38	0.43	0.39	-0.17	-0.47	-0.31	**0.85**	0.52
PerBen2	0.38	0.38	0.33	0.33	0.36	0.37	-0.11	-0.38	-0.33	**0.84**	0.53
PerBen3	0.47	0.38	0.35	0.35	0.37	0.40	-0.12	-0.41	-0.32	**0.84**	0.55
PerBen4	0.42	0.38	0.37	0.35	0.35	0.36	-0.16	-0.42	-0.34	**0.84**	0.49
int1	0.53	0.53	0.55	0.48	0.52	0.50	-0.19	-0.57	-0.52	0.53	**0.90**
int2	0.52	0.55	0.57	0.55	0.54	0.49	-0.14	-0.55	-0.53	0.61	**0.91**
int3	0.44	0.48	0.50	0.46	0.46	0.50	-0.16	-0.45	-0.56	0.51	**0.84**

Table 3. Loadings and cross loadings of latent variables

5.2 Structural model analysis

The structural model was estimated for hypotheses significance and explanatory power. Table 4 presented the results of the model assessment, including standardized path coefficients, significance of the paths. As we can see, H2, H3, H4, H5, H6, H9, H10 were supported, while H1, H7, H8 were not. Besides, our model explained 68.2% of the total variance in employees' intention to Internet abuse.

Hypotheses	Path Coefficients	t-value	p-value
H1: Denial of responsibility →Internet abuse intentions	0.061	1.600	n.s.
H2: Denial of injury →Internet abuse intentions	0.111**	2.854	P<0.01
H3:Denial of victim→Internet abuse intentions	0.174***	4.486	P<0.001
H4: Condemnation of the condemners →Internet abuse intentions	0.110**	2.968	P<0.01
H5:Appeal to higher loyaltyies→Internet abuse intentions	0.106**	2.838	P<0.01
H6: Claim of relative acceptability→Internet abuse intentions	0.120**	3.247	P<0.01
H7:perceived severity of sanction →Internet abuse intentions	0.056	1.933	n.s.
H8:Perceived certainty of detection →Internet abuse intentions	-0.003	0.055	n.s.
H9:Perceived security risks→Internet abuse intentions	-0.249***	4.524	P<0.001
H10:Perceived benifits →Internet abuse intentions	0.232***	6.744	P<0.001

Table 4. Path Loadings and T Values

6 DISCUSSIONS AND IMPLICATIONS

6.1 The Role of neutralization in Internet abuse

As expected, we find that neutralization techniques are excellent antecedents of employees' intention to Internet abuse except denial of responsibility. This finding is in accord with neutralization studies in other areas. Previous research in Criminology has found that neutralization techniques explain deviant actions in a military environment (Pershing, 2003), computer hacking (Morris 2010), corporate crime (Piquero et.al. 2005), and cannabis use (Patrick P.W. 2003). In software piracy study, Siponen, et al. (2012) proposed a theoretical model in which the effects of neutralization techniques are tested alongside different types of deterrents on software piracy intentions. Results showed that

two kinds of neutralization techniques, appeal to higher loyalties and condemnation of the condemners influencing employees' intentions to software piracy. Hinduja (2007) studied the influences of nine neutralization techniques on software piracy, and the results suggested four techniques have positive effects on the outcome variable –Denial of Injury, Appeal to Higher Loyalties, Denial of Negative Intent, and Claim of Relative Acceptability. Based on our findings, Denial of injury, Denial of victim, Condemnation of the condemners, Appeal to higher loyalties, Claim of relative acceptability strongly increased the intention to Internet abuse. These are new predictors of Internet abuse. To make it more difficult for employees to rationalize the deviant and costly act of Internet abuse, we suggest Internet usage policy awareness campaigns and educational sessions on neutralization need to be examined in order to identify effective means of challenging the use of neutralization techniques and thus curb Internet abuse in the workplace.

6.2 The Role of rational choice theory in Internet abuse

As for the influence of cost-benefits analysis, our data suggest that formal sanctions do not predict Internet abuse intentions. While this finding is different from empirical studies in IS security practices (D'Arcy, et al., 2009; Kankanhalli, et al., 2003; Li, et al., 2009), it is consistent with a study that applied neutralization techniques in the field of security policies violations (Siponen & Vance, 2010; Siponen, et al., 2012). A possible explanation for the different results is that neutralization techniques enable people to act rule-breaking behaviours, while at the same time enabling them to view themselves as no default in general (Sykes & Matza, 1957). Another reason may be that some of the employees are not aware of the sanctions about Internet abuses. The results indicate that in Internet usage management practices, organizations need to give a clear declaration of the punishments about Internet abuse behaviours and implement the policy strictly.

What's more, based on the above results, perceived security risks and perceived benefits have found significantly related to employees' Internet abuse intentions. These means that employees are generally aware that Internet abuses may bring ones' computer and information into security breaches, but the benefits from Internet abuse outweigh the security threats.

6.3 Implications for research and practice

From a researcher's perspective, since first proposed by Sykes and Matza (1957), neutralization theory has been widely applied in many areas. Results of our study indicate that the theory can also be used to solve IS security issues in the workplace in future organizational behaviour research. What's more, the present study also brings about another research stream on how best to inhibit the use of neutralization techniques. From a practitioner's perspective, our findings suggest that managers need to understand and fully appreciate the cognitive processes underlying the occurrence of Internet abuse in their organizations. For one aspect, managers can control employees' usage of neutralization strategies by treating employees fairly, raising employees' awareness of potential damage to the organization if they commit personal Internet usage deeds in the workplace. What's more, ensuring that employees understand that hard work for the company does not give them justification to Internet abuse during working hours. For another aspect, although the effect of sanctions was not significant to employees Internet abuse intentions in our analysis, it does not mean that formal sanctions are not effective deterrents. Employers should give a clear definition of the sanction of Internet abuse and implement the rule strictly so as to increase the cost of personal Internet usage and reduce relative deviant actions. Anyway, managers need to make sure that the Internet works for, but not against the organization.

6.4 Limitations and future research

A key limitation of our study should be addressed in future work is the sample. First, although part of the participants in our study completed a pen-and-paper survey, the others who filled out an online survey may cause respondent bias (Lim, 2002). It was contended that subjects who respond to online questionnaires tend to be more Internet-savvy, and are hence more prone to commit Internet abuses in the first place. Second, in our survey, part of the respondents reported that there is no clear declaration

of Internet usage policies or they are not aware of the policies, which means that they are not aware of the formal sanctions of Internet abuse. Those persons should have separately study with a control study of respondents with organizational Internet usage policies.

7 CONCLUSION

Many organizations have scrambled to get control measures and discipline mechanisms in place to deter employees from engaging in Internet abuse. Since control measures and discipline systems are insufficient to curb Internet abuse at the workplace, we propose to integrate the control perspective with neutralization techniques and cost-benefit analysis. Although qualified by several limitations, the results of this study suggest that most of the neutralization techniques significantly influence employees' intentions to Internet abuse. Our study, therefore, highlights neutralization as an important factor to take into account with regard to developing and implementing organizational Internet usage policies and practices. The empirical results of our paper also suggest the importance of taking the benefit and security risk factors into account when regulating employees' Internet abuse behaviours.

Acknowledgment

This work is partially supported by the National Natural Science Foundation of China under Grant No. 70972058，71272092. We thank the editor and the reviewers for their comments and suggestions.

Appendix. Survey instrument

Construct	Item	
Internet Abuse Intention	int1	I intend to use Internet provided by the organization for non-work-related purposes in the future.
	int2	I will use Internet provided by the organization for non-work-related purposes in the future.
	int3	I expect to use Internet provided by the organization for non-work-related purposes in the future.
Perceived certainty	Cert1	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).
	Cert2	I would probably be caught.
Perceived severity	Sev1	If I were caught using the Internet access provided by the organization for non-work-related purposes, I think the punishment would be (Very Low/Very High).
	Sev2	I would be severely punished by my organization.
	Sev3	My Internet access privileges being restricted by the organization.
Perceived Security Risk	PerSec1	At my workplace, the risk to my computer and data from Internet security breaches is (Very Low/Very High).
	PerSec2	At my workplace, the chance that my computer will fall a victim to an Internet security breach is (Very Low/Very High).
	PerSec3	Internet abuse might increase an organizations' exposure to security risk.
	PerSec4	Internet abuse might increase the risk of confidential information leaking.
Perceived Benefit	PerBen1	Using the Internet access provided by the organization for non-work-related purpose will result in Saving my personal time using private Internet access.
	PerBen2	Saving my personal expense using private Internet access.
	PerBen3	Convenience.
	PerBen4	More interesting work life.
Denial of responsibility	It is OK to use the Internet access provided by the organization for personal purposes if …	
	DenRes1	my daily tasks and job objectives is not distributed clearly.
	DenRes2	the internet use policy is not explicitly advertised.

	DenRes3	the work stress is too high.
Denial of injury	DenInj1	no harm is done.
	DenInj2	no damage is done to the company.
	DenInj3	no one gets hurt.
Denial of victim	DenVic1	if the managers are worried about harm from internet abuse they should have better online management.
	DenVic2	I don't really buy into the idea that the company loses much from internet abuse.
	DenVic3	it is OK to surf the net for non-work reasons because my boss is biased and does not treat us well.
Condemnation of the condemners	ConCon1	managers should be more worried about other kinds of misconducts than internet abuse.
	ConCon2	the Company where I work really should worry about other issues than internet abuse.
	ConCon3	the Company has been ripping our employees off for years, so internet abuse is justified.
Appeal to higher loyalties	AppHLoy1	If it is used to benefit an individual or a business somehow?
	AppHLoy2	It is all right to use the Internet access provided by the organization for personal purposes to get my work done more efficiently.
	AppHLoy3	If a family member, friend, or significant other needed me to do such thing.
Claim of relative acceptability	ClReAcc1	Because the anonymous nature of the Internet affords privacy and somewhat of a shield from detection; and so, why not take advantage?
	ClReAcc2	Because no one really cares about what I do online – it is just too removed from the real world?
	ClReAcc3	Because it is better, or at least more acceptable, to be engaging in this activity than going out and tangibly harming people?

References

Al-Saad, A., & Saleh, Z. (2011). Identifying Internet Abuse by Analyzing User Behavior on the Internet. Journal of Internet Banking and Commerce, 16(1), Special Section p1.

Bloxx. (2008). Productivity, Internet abuse, and how to improve one by eliminating the other. In: http://www.bloxx.com/assets/downloads/bloxx_whitepaper_productivity.pdf.

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

Bock, G.W., Kuan, H.H., Liu, P., & Sun, H. (2007). The role of task characteristics and organization culture in non-work related computing (NWRC). In Human-Computer Interaction, Part I, HCII 2007, Jacko J., Editor. Springer-Verlag: 681-690.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523-548.

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

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.

Garrett, R.K., & Danziger, J.N. (2008). 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.

Henle, C.A., & Blanchard, A.L. (2008). The interaction of work stressors and organizational sanctions on cyberloafing. Journal of Managerial Issues, 383-400.

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

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.
Lee, O.K.D., Lim, K.H., & Wong, W.M. (2005). Why employees do non-work-related computing: An exploratory investigation through multiple theoretical perspectives. In (pp. 185c-185c): IEEE.
Lee, S.M., Lee, S.G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707-718.
Lee, S.M., Yoon, S., & Kim, J. (2008). The Role of Pluralistic Ignorance in Internet Abuse. Journal of Computer Information Systems, 48(3), 38-43.
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.
Lim, V.K.G., & Teo, T.S.H. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. Information & Management, 42(8), 1081-1093.
Lim, V.K.G., Teo, T.S.H., & Loo, G.L. (2002). How do I loaf here? Let me count the ways. Communications of the ACM, 45(1), 66-70.
Mahatanankoon, P., Anandarajan, M., & Igbaria, M. (2004). Development of a measure of personal web usage in the workplace. CyberPsychology & Behavior, 7(1), 93-104.
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. C.A. Simmers (ed.), Information Science Publisher, Hershey, PA, 111-124.
Morris, R. G. (2010). Computer Hacking and the Techniques of Neutralization: An Empirical Assessment. Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications: 1-17.
Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: testing a rational choice model of corporate crime. Law & Society Review, 30(3), 549-584.
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.
Piquero, N.L., Tibbetts, S.G., & Blankenship, M.B. (2005). Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime. Deviant Behavior, 26(2), 159-188.
Rajah, R., & Lim, V.K.G. (2011). Cyberloafing, Neutralization and Organizational Citizenship Behavior. In PACIS.
Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.
Siponen, M., Vance, A., & Willison, R. (2012). New Insights into the Problem of Software Piracy: The Effects of Neutralization, Shame, and Moral Beliefs. Information & Management.
Spy., S. (2011). Employee Computer & Internet Abuse Statistics. In. http://www.snapshotspy.com/employee-computer-abuse-statistics.htm.
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. (2007). Exploring Internet abuse in the workplace: how can we maximize deterrence efforts? Review of Business Journal.
Velezmoro, R., Lacefield, K., & Roberti, J.W. (2010). Perceived stress, sensation seeking, and college students' abuse of the Internet. Computers in Human Behavior, 26(6), 1526-1530.
Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. Computers in Human Behavior, 27, 1751–1759.

Woon, I.M.Y., & Pee, L.G. (2004). Behavioral factors affecting Internet abuse in the workplace: an empirical investigation. In Proceedings of the Third Annual Workshop on HCI Research in MIS, Washington, D.C., December 10-11: 80-84.

Woon, I.M.Y., Tan, G.W., & Low, R.T. (2005). A protection motivatoin theory approach to home wireless security. In Proceedings of the Twenty-Sixth International Conference on Information Systems. Las Vegas.

Young, K. (2010). Policies and procedures to manage employee Internet abuse. Computers in Human Behavior, 26(6), 1467-1471.

Young, K.S. (1996). Addictive use of the internet: a case study that breaks the stereotype. Psychological Reports, 79, 899-902.

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