

A Moral-Belief Model for Deterring Non-Work-Related Computing in Organizations

Tserendulam Munkh-Erdene^a, Sang Cheol Park^{b,*}

^a Graduate Student, Department of Business Administration, Daegu University, Korea

^b Assistant Professor, Department of Business Administration, Daegu University, Korea

ABSTRACT

Negative consequences incurred from employees' non-work-related computing (NWRC) have been one of the security-related issues in information intensive organizations. While most studies have focused on the factors that motivate employees to engage in NWRC, this study examines the mediating effect of moral beliefs on the relationship between sanctions and NWRC using a moral beliefs-based model. The research model posits that the formal (i.e., punishment severity and detection certainty) and informal sanctions (subjective norms and descriptive norms) enhance employees' moral beliefs against NWRC intention. From a cross-sectional scenario-based survey involving 176 employees working at banks in Mongolia, our results indicate that moral beliefs fully mediate the relationship between detection certainty/subjective norms and NWRC intention and act as a partial mediator in the relationship between descriptive norms and NWRC. The findings from this study present empirical evidence that both informal and formal sanctions could be an effective deterrent for NWRC intention through employees' moral beliefs.

Keywords: Non-Worked-Related Computing, Punishment Severity, Detection Certainty, Subjective Norms, Descriptive Norms, Moral Beliefs

I . Introduction

Nowadays, information and communication technology (hereafter, ICT) is predominantly used in every aspect of our lives. Employees use ICT for personal purposes during work hours despite company policies which prohibit such behavior. Such behavior is called non-work-related computing

(hereafter, NWRC) (Bock and Ho, 2009). Prior studies have indicated that NWRC results in negative productivity, bandwidth degradation, information leaking, and risk of legal liability to organizations (Cheng et al., 2014; Khansa et al., 2017). Moreover, industry surveys among managers showed that NWRC leads to information systems risks (Statista, 2015; World Economic Forum, 2018). Thus, although

*Corresponding Author. E-mail: scpark77@daegu.ac.kr Tel: 82538506276

NWRC is considered a minor issue compared to other IS security issues, individuals' unintentional act in organizations could be the precursor to more extreme issues.

As a precursor to IS security issues, studies in the IS field have investigated how to deter NWRC by employing organizational policies such as formal sanctions (Cheng et al., 2014; Khansa et al., 2017). In a similar vein, Cheng et al. (2014) have suggested that detection certainty of formal sanctions could deter employees' NWRC intention, even if they rationalize their own behavior. Khansa et al. (2017) have investigated how employees rationalize their behavior before and after the formal announcement of organizational controls, and found that employees only rationalize when they are aware their behavior is wrong, suggesting that formal control could backfire by increasing the occurrence of NWRC. These findings put the effectiveness of formal sanctions in doubt.

To effectively enforce work policies, prior works in the criminology, social psychology, and ISS fields have shown the importance of moral beliefs, which promotes compliance with laws, regulations, and policies (D'Arcy and Devaraj, 2012; Hu et al., 2011; Li et al., 2010; Schoepfer and Piquero, 2006). Despite the importance of moral beliefs in discouraging IS security-related behavior, extant research has not fully examined what role the moral beliefs play to deter NWRC. Moral beliefs refer to employees' judgments of rightness about specific behaviors (Bachman et al., 1992) and drive one to comply, or not to comply, with rules and regulations. As implementing formal sanctions incurs inefficient costs for organizations if employees do not follow or act in accordance with those policies, in the long run, it is important to engage employees in compliance behaviors even in the absence of formal

sanctions.

Therefore, it is essential to gain a better understanding of how moral beliefs affect NWRC along with formal and informal sanctions which are common countermeasures to prevent ISS policy violation. To examine mediating relationships of moral beliefs on the two types of sanctions and NWRC, this study integrates key constructs from general deterrence theory (Gibbs, 1975), theory of planned behavior (Ajzen, 1991), and law legitimacy theory (Tyler, 2006). To examine formal sanctions, this study applies general deterrence theory (Gibbs, 1975), which explains how perceptions of punishment severity and detection certainty constrain NWRC. Besides formal sanctions, informal sanctions play an important role in organizational culture and deter employees' NWRC. Through the application of the theory of planned behavior, this study examines how subjective and descriptive norms negatively influence NWRC. Finally, this study examines how moral beliefs motivate employees to comply with formal and informal sanctions from the law legitimacy theoretical perspective (Tyler, 2006).

The purpose of the current study is to investigate the effects of formal and informal sanctions through moral beliefs by deriving constructs from different theories which have been widely adopted in IS security research. It aims to reveal the underlying cognitive processes which explain how moral beliefs prevent employees from engaging in NWRC.

Based on the above arguments, this study seeks to answer the following research questions:

1. *What role do moral beliefs play in deterring NWRC within organizations?*
2. *How do employees' perception of formal and informal sanctions results in reduced NWRC intention in organizations through their moral beliefs?*

This research is expected to contribute significantly to the NWRC literature both theoretically and practically. Theoretically, this study develops a moral beliefs-based model for exploring methods to deter NWRC in organizations. More specifically, this study presents empirical evidence that moral beliefs could play a mediating role in the relationships between the two types of sanctions (i.e., formal and informal sanctions) and NWRC. Practically, this study suggests that practitioners should focus on the importance of moral beliefs for deterring NWRC in organizations. Based upon the empirical results in this study, managers interested in decreasing NWRC should establish more sophisticated ICT policies.

The rest of this paper proceeds as follows. It begins with a literature review and theories underlying the research model. Next, the research hypotheses pertaining to the mediating role of moral beliefs on the relationship between sanctions (i.e., formal and informal sanction) and NWRC are developed. This is followed by research methodology and data analysis. Finally, it highlights the implications for research and practice, as well as the limitations of the findings along with suggested directions for future research.

II. Theoretical Background

This study integrates constructs from law legitimacy theory, deterrence theory, and theory of planned behavior to identify methods to deter NWRC in organizations. In order to prevent deviant and counterproductive behaviors, organizations formulate a series of policies and rules which construct the rightness of behaviors. In a similar vein, most organizations have procedures which prohibit NWRC. Thus, general deterrence theory, one of the

most widely applied theories in the IS domain (D'Arcy and Herath, 2011; Guo et al., 2011; Herath and Rao, 2009b; Hu et al., 2011; Straub, 1990), is adopted to investigate how formal sanctions could constrain employees from NWRC. In addition to formal sanctions, informal sanctions play an important role in organizational culture and deterrence of employees' deviant acts. Prior research in the IS security field has investigated the effects of subjective and descriptive norms as informal sanctions from theory of planned behavior (Herath and Rao, 2009b; Khansa et al., 2017; Yazdanmehr and Wang, 2016). These norms encourage people to be law abiding. Thus, this study integrates two constructs derived from the theory of planned behavior in order to examine how informal sanctions impede NWRC. Although prior studies have indicated that both formal and informal sanctions may deter deviant behavior or encourage compliance behavior to a certain level, some people still engage in NWRC. Law legitimacy theory (Tyler, 2006) suggests that personal moral beliefs motivate people to follow rules and act as a self-regulation of their own behavior in accord with one's sense of what is appropriate and right to do in a given situation. The following parts explain each construct based on each theory.

2.1. Literature Review on NWRC

In prior research, the terms "cyberloafing" and "non-work-related computing" (hereafter, NWRC) have been used interchangeably (Cheng et al., 2014; Khansa et al., 2017), although they differ slightly in some ways. In their preliminary research, Kim and Byrne (2011) studied and distinguished the conceptualization of the behaviors associated with Internet users' behavior - surfing online for non-work-related purposes while supposedly working.

The distinct characteristics between cyberloafing and NWRC are: (1) NWRC is a broader concept than cyberloafing, and (2) NWRC is purposeful while cyberloafing is aimless and undirected. Despite the above mentioned differences, these terms bear the following similarities (1) in both cases, employees use resources provided by organizations for their personal tasks despite their purpose, and (2) both behaviors incur negative repercussions for organizations, such as losses in productivity that affect a company's financial performance, increase in vulnerabilities and exposure to security risks, as well as illegally accessing pirated material. Thus, most studies have used the two concepts interchangeably. This study defines NWRC as an employee's behavior that uses an organization's ICT resources during work hours for personal purposes.

Due to the similarity, the current research has analyzed both the cyberloafing and the NWRC literature. Prior research has investigated both antecedents (Khansa et al., 2017; Lim, 2005) and consequences (Bock and Ho, 2009; Kuem and Siponen, 2014) of NWRC. In the case of an overarching theory to explain NWRC, previous studies have employed a variety of theories such as rational choice perspective (Cheng et al., 2014), general deterrence theory (Cheng et al., 2014), theory of planned behavior (Pee et al., 2008), neutralization theory (Cheng et al., 2014; Khansa et al., 2017; Lim, 2005), and theory of interpersonal behavior (Pee et al., 2008).

In terms of consequences, studies have found that low cognitive, short-time NWRC such as surfing the Internet or using social media, enables employees to recover their energy, which in turn positively influences their creative performance. However, high cognitive NWRC including writing emails, making online purchases or spending much time on NWRC leads to a decrease in performance (Bock and Ho,

2009; Kuem and Siponen, 2014; Lim and Chen, 2012).

Although prior studies have emphasized both negative and positive impacts of NWRC, more extreme issues could stem from one employee's unintentional act. For instance, employees could use organizational ICT resources in order to upload files to a USB (consequence: threat of unrecognized viruses), or an employee conducts online banking transactions to make an online purchase (consequence: security concern). Therefore, it is essential to examine how to impede employees' NWRC in organizations.

Previous research in the IS security field has recommended implementation of policy as the most common and effective means to curb employees NWRC (Cheng et al., 2014; D'Arcy and Devaraj, 2012; Herath and Rao, 2009b; Willison and Warkentin, 2013). In a NWRC context, Cheng et al. (2014) conducted research on the personal use of Internet at work. They examined the effects of sanction severity, detection certainty, perceived benefit, and neutralization techniques on intention to use the Internet for personal purposes via surveys among 230 employees working in Chinese companies. Their findings suggest that detection certainty could deter intention to use the Internet for personal reasons, even in the presence of neutralization. Khansa et al. (2017) have investigated how employees neutralize their intention before and after the formal announcement of organizational control on cyberloafing via a longitudinal survey ($n = 360$). They claimed that people only neutralize when they are aware that their behavior is wrong. These findings suggest that predictors of cyberloafing behavior change depending on the announcement of formal controls. While studies in the IS security field have recommended both formal and informal sanctions as countermeasures to curb IS-related deviant behaviors, our review showed that prior studies concerning NWRC have not fully exam-

ined deterrence factors. Therefore, this study aims to test the deterrence effects of various factors.

2.2. Moral Beliefs from Law Legitimacy Theory

Law legitimacy theory (hereafter, LLT) provides a framework for understanding how people comply with laws and rules voluntarily (Tyler, 2006). In his theory, Tyler suggests two approaches to encourage rule-following, including the command-and-control approach and the self-regulatory approach (Tyler and Blader, 2005). The command-and-control approach takes into account extrinsic motivation, which represents people's responses to external contingencies in their environment. Conversely, the self-regulatory approach is linked to intrinsic motivation, which is based on the individuals' intrinsic desires or feelings of personal obligation. Tyler and Darley (2000) have identified two intrinsic motivational forces, or social value judgments for rule-following: legitimacy and morality. Legitimacy refers to the judgment about whether the organization has the authority to enforce policies. Morality refers to the judgment of the rightness or wrongness of specific behaviors. Supporting the LLT, Hunt and Vitell (1986)'s ethical decision making theory posits that the inherent evaluation of the behavior affects a person's decision to take action or not.

LLT was originally developed to examine why citizens do not follow laws and how to encourage law-abiding behavior (Tyler, 2006). According to LLT, the presence of a law enhances perception of the appropriateness of behavior (D'Arcy and Devaraj, 2012; Tyler and Blader, 2005). Recently, IS security studies have adopted a "morality" component in order to interpret why employees comply with IS security policy or engage in IS-related deviant behavior in the presence of IS policy (D'Arcy and Devaraj,

2012; Li et al., 2014; Li et al., 2010; Thong and Yap, 1998; Xu et al., 2016). These studies have conceptualized this construct as "moral beliefs" or "personal norms" and operationalized the construct as an individual's judgment of right or wrong regarding the behavior of interest. Moral beliefs have been demonstrated to be critical in controlling many types of deviant behaviors. Thong and Yap (1998) and Moores and Chang (2006) found that moral beliefs are effective in preventing infringement of intellectual property rights and theft of digital goods (e.g., software piracy). Li et al. (2010) suggested that organizational context factors (e.g., organizational norms and identification) positively influence personal norms. Organizational norms, as a type of social norm, can be an important information source for individuals in shaping their personal moral views and can be internalized as part of an individual's personal norms. If most people in an organization are not tolerant of Internet abuses, an individual employee in the organization is more likely to form personal norms against Internet abuses.

In meantime, moral beliefs have been defined as an individual's judgment of right or wrong about specific behaviors (Bachman et al., 1992; D'Arcy and Devaraj, 2012). In IS security research, personal norms (Li et al., 2010), personal ethical norms (Li et al., 2014), information security policy-related personal norms (Yazdanmehr and Wang, 2016), and moral beliefs (D'Arcy and Lowry, 2017) are viewed as personal standards. Distinct roles of moral beliefs have been studied in the criminological, psychological, and ISS fields (Li et al., 2014; Schoepfer and Piquero, 2006; Strelan and Boeckmann, 2006). <Table 1> presents brief descriptions and assumptions of the moral beliefs.

From a predictor perspective, Hu et al. (2011) examined whether self-control, moral beliefs, and

<Table 1> Roles of Moral Beliefs

Roles	Definitions	Arguments	Studied relationships
Predictor	A stable, individual difference construct	Moral beliefs have a strong negative effect on deviant or criminal behavior	Perceived informal risk calculus (Hu et al., 2011)
Moderator		Effects of an individual's self-control and other external controls on his/her behavioral intention are contingent upon the strength of his/her moral beliefs against the deviant or criminal act	In the relationship between self-control and criminal behaviors (i.e., assault and theft) (Schoepfer and Piquero, 2006) In the relationship between sanction severity and Internet use policy compliance (Li et al., 2010)
Mediator	An individual judgment of specific behavior, influenced by situational aspects	Moral beliefs can be developed through environmental perceptions and are defined in terms of judgments and evaluations of the act	Legal sanctions and use of the performance-enhancing drug (Strelan and Boeckmann, 2006) Formal sanctions, social desirability pressure and misuse of IT resources (D'Arcy and Devaraj, 2012) The effectiveness of community anti-aggression policy, peer pressure against aggression, face-saving and Internet aggression in an online community (Xu et al., 2016)

deterrence predict intention to comply with information security policy. They concluded that deterrence does not sufficiently reduce policy violating intention, and moral beliefs have a stronger negative effect on perceived informal risk calculus. Prior research in different disciplines has demonstrated the moderating role of moral beliefs in the relationship between self-control and criminal behavior, as well as sanction and Internet use policy compliance intention. The studies in this stream argue that the effects of an individual's self-control and other external controls on their behavioral intention are contingent upon the strength of their moral beliefs against the deviant act (Li et al., 2010; Schoepfer and Piquero, 2006). Schoepfer and Piquero (2006) found that moral beliefs act as a moderator in the relationship between self-control and criminal behavior (i.e., assault and theft). They conducted a survey among 300 undergraduate students in order to examine how individuals' low self-control and high moral beliefs inhibit their criminal behaviors. Results showed that self-control, moral beliefs, and criminal behavior are interrelated; that is, individuals with low self-control

have weak moral beliefs against those acts. In the ISS area, Li et al. (2010) have examined the moderating effect of personal norms¹⁾ in the relationship between detection probability/sanction severity and intention to comply with Internet use policy. They found that when employees have strong morality against the deviant behavior, the effects of detection probability and sanction severity are overridden.

However, some studies have shown that moral beliefs may act as a mediator rather than a moderator due to their variance depending on the situation. While the moderator perspective conceptualizes moral beliefs as an organized and fully developed ethical system (D'Arcy and Devaraj, 2012; Paternoster and Simpson, 1996), from the mediator perspective, moral beliefs refer to one's moral evaluation of a behavior within a particular context. In the social psychological area, Strelan and Boeckmann (2006) elucidated how and why personal moral beliefs play a mediating role in the relationship between legal sanctions and athletes' use of performance-enhancing drugs. Results

1) Personal norms, personal ethics, ethical beliefs, and moral beliefs are same constructs in studies cited here.

show that legal sanctions transfer information about appropriateness of the behavior, forming perceptions of the rightness of the behavior. In the ISS research field, D'Arcy and Devaraj (2012) studied how formal sanctions and social desirability pressure enhance moral beliefs and deter the misuse of IT resources. They conducted a scenario-based survey among two groups of participants, a sample of employees ($n = 228$) and a sample of employed professionals taking MBA classes ($n = 183$). Their results indicate that moral beliefs partially mediate the relationship between formal sanctions/social desirability pressure and intention of technology misuse. Xu et al. (2016) investigated effects of deterrence factors, such as the effectiveness of community anti-aggression policy, peer pressure against aggression, moral beliefs, and face saving on Internet aggression behavior among Chinese online social network community users ($n = 322$). They found that both effectiveness of community anti-aggression policy and peer pressure against aggression indirectly influence Internet aggression intention, suggesting that these two factors decrease aggression behavior by enhancing community members' moral beliefs against aggression. While prior studies have solely investigated the formal sanctions as a second-order construct, this study examines the effects of severity and certainty separately, as investigating the relative importance of different characteristics of formal sanctions may give direction for managers to design sanctions more effectively. While there is controversy concerning the role of moral beliefs in many different research contexts, this study has adapted the construct "moral beliefs" as a mediator. This is because NWRC is a context-specific behavior - that is, the behavior is not an acceptable behavior within organizations. In short, we have argued that employees' moral beliefs may stem from formal and informal sanctions which clar-

ify whether NWRC is considered wrong behavior and to what extent a behavior is not tolerated.

2.3. Formal and Informal Sanctions

In this study, we have presented the General deterrence theory (hereafter, GDT) to explain formal sanctions. It has been one of the representative theories in criminology used to examine illicit, deviant, and antisocial behaviors. Deterrence is defined as "the preventive effect which actual or threatened punishment of offenders has upon potential offenders" (Gibbs, 1975). GDT posits that individuals are rational and weigh costs and benefits when deciding whether to obey existing laws, rules and norms. It focuses on formal sanctions against committing a criminal act and their effectiveness as a deterrent. According to GDT (Gibbs, 1975), the effectiveness of sanctions is based on certainty, severity, and celerity. Certainty means that an individual believes that his or her criminal behavior will be detected, while severity means the degree to which it will be punished. Celerity refers to how quickly the punishment occurs following the criminal act.

GDT has been applied to numerous research contexts, including general criminal context as well as employees' deviant behaviors. In organizational contexts, sanctions are more effective to inhibit employees from committing deviant behaviors because employees usually conform to rules and regulations (Straub, 1990).

Since its initial adoption in the IS security field, GDT has been widely adopted to examine IS security-related behaviors, such as Internet aggression (Xu et al., 2016), IS policy compliance (Herath and Rao, 2009b; Li et al., 2014; Li et al., 2010; Straub, 1990), employee IS misuse (D'Arcy and Devaraj, 2012; Nagin and Pogarsky, 2001), cyberloafing (Cheng et

al., 2014). Prior studies have often conceptualized and investigated formal sanctions in terms of certainty and severity (Herath and Rao, 2009a; Li et al., 2010; Xu et al., 2016). For example, Herath and Rao (2009a) investigated how the severity of penalty and the certainty of detection encouraged IS policy compliance intention with a sample of 312 employees working in 77 organizations in the US. Their results suggested that certainty of detection has a positive impact on compliance intention whereas punishment severity negatively influences compliance intention, indicating that penalties which are too severe could disrupt employees' cooperative behavior. On the contrary, Li et al. (2010) and D'Arcy et al. (2009) found that perceived certainty and severity of formal sanctions are effective in deterring IS-related deviant behaviors. Based on the above studies, the current research adopts the severity and certainty components of GDT and hypothesizes that both components play deterrence roles.

In the NWRC context, this study assumes that severe punishment and high detection certainty send signals to employees of organizational efforts to monitor, evaluate, and punish these behaviors. Consequently, employees are expected to view the behavior as morally wrong and be less likely to engage in NWRC.

Meanwhile, in regard to informal sanctions, this study has attempted to consider the Theory of planned behavior (hereafter, TPB). It is one of the most influential theories for the prediction of social behaviors (Ajzen, 1991). TPB posits that individuals' attitudes and subjective norms as well as their perceived behavioral control positively influence their behavioral intention which lead to their own behavior.

TPB has been widely applied in the IS literature, including in a security context (Herath and Rao, 2009b; Pee et al., 2008). Pee et al. (2008) compared

alternative models, theory of interpersonal behavior (TIB) and TPB, for explaining NWRC. They tested these models with data of 214 employees. Their results indicated that both theories significantly predict NWRC, and TIB explained greater variance in NWRC. Most importantly, Pee et al. (2008) found social factors including the expectations of coworkers, friends, and IT departments were the most important factors in decreasing NWRC. Herath and Rao (2009b) integrated organizational commitment, protection motivation theory and deterrence theory under the umbrella of TPB to explain employees' motivation to comply with security policy. They conducted the study using 312 respondents from 78 organizations in the US and found that organizational commitment, self-efficacy, subjective norms, descriptive norms, and detection certainty are significant motivators for security policy compliance intention. As evident from prior research in the IS security context, social factors such as subjective norms and descriptive norms are one of the salient factors which predict inappropriate behavior in the workplace.

Among these constructs, subjective norms refer to TPB. However, Sheeran and Orbell (1999) suggested in their study to include descriptive norms as an additional normative predictor for TPB. They claim that descriptive norms are the "is" norm which refers to the perceptions of other people's behavior in the domain while subjective norms (i.e., injunctive norms) are the "ought" norm which is defined as the perceived social pressure of whether or not to engage in a behavior (i.e., what other people think that one ought to do). These norms are distinct sources of motivation.

Based on prior studies and Sheeran and Orbell (1999)'s augmented theory of planned behavior, this study adopts subjective norms and descriptive norms from TPB to investigate how to deter NWRC in

organizations. Consistent with TPB, recent studies based on GDT have adopted both subjective and descriptive norms as informal sanctions. In the context of NWRC, subjective and descriptive norms exert social influence or pressure which can shape employees' moral beliefs toward the use of ICT resources within the organization.

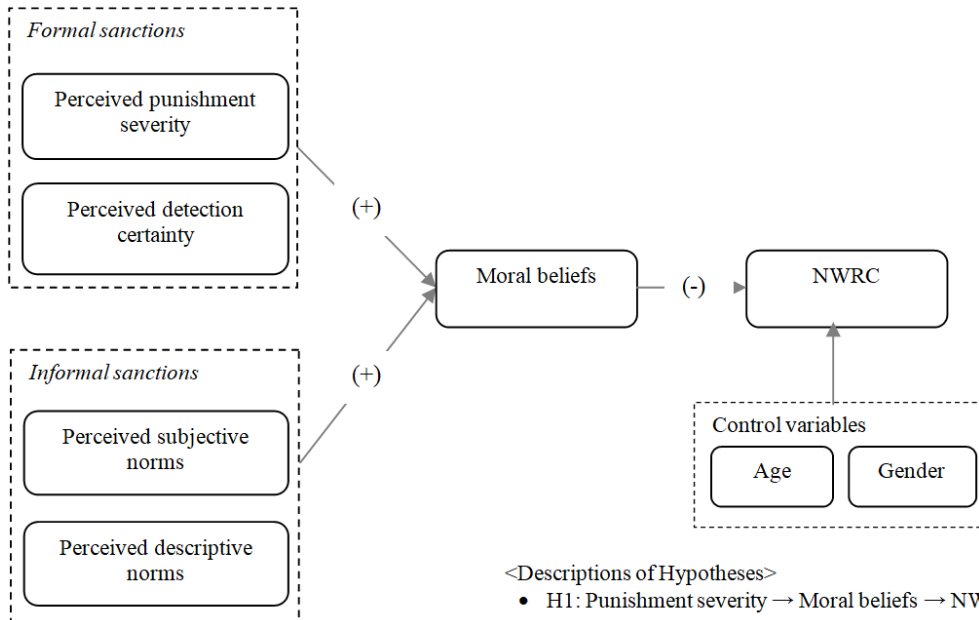
III. Research Model and Hypotheses Development

3.1. Research Model

<Figure 1> illustrates the proposed research model. As shown in the model, both formal and informal sanctions are posited to have indirect effects on NWRC by mediating moral beliefs. We have further

considered both age (Everton et al., 2005), and gender (Cheng et al., 2014; Everton et al., 2005; Herath and Rao 2009b; Magnuson and Dundes, 2008; Vitak et al., 2011) as control variables which may influence the NWRC in organizations.

Punishment severity and detection certainty are adapted from general deterrence theory, whereas subjective norms and descriptive norms derive from the theory of planned behavior. In organizational settings, rules and norms shape what is right and wrong. Therefore, these four constructs may trigger the rightness of the behavior and detract from the moral beliefs opposing the behavior. In turn, moral beliefs act as countermeasures to NWRC. In this study, moral beliefs refer to employees' judgments or evaluations of right and wrong regarding NWRC (Bachman et al., 1992).



<Descriptions of Hypotheses>

- H1: Punishment severity → Moral beliefs → NWRC
- H2: Detection certainty → Moral beliefs → NWRC
- H3: Subjective norms → Moral beliefs → NWRC
- H4: Descriptive norms → Moral beliefs → NWRC

<Figure 1> Research Model

3.2. Research Hypotheses

Sanctions refer to the threatened penalty for a deviant act (Gibbs, 1975). There are formal and informal sanctions in organizations, which inform the appropriateness of acts (Cheng et al., 2013). While formal sanctions are formally documented rules and procedures which are initiated by management, informal sanctions refer to social censure which is unwritten and often initiated by employees themselves.

According to general deterrence theory (Gibbs, 1975), formal sanctions have three components: certainty, severity, and celerity. If an individual perceives that the certainty, severity, and celerity of sanctions are high, they will not engage in a criminal act. Prior studies have predominantly conceptualized and investigated formal sanctions in terms of certainty and severity (Cheng et al., 2014; Li et al., 2014). In their review and analysis of deterrence theory, D'Arcy and Herath (2011) found that deterrence studies have rarely included celerity of sanctions due to measurement difficulties and lack of theoretical importance. Celerity of sanctions represents how quickly punishment occurs (Nagin and Pogarsky, 2001). According to Nagin and Pogarsky (2001), celerity effects depend on the person's preferences for the timing of penalties – present-oriented or future-oriented. In organizational contexts, delayed punishment rarely occurs. Thus, in this study, formal sanctions consist of two dimensions: punishment severity and detection certainty following prior studies in the IS field.

Informal sanctions, on the other hand, consist of subjective and descriptive norms in this study. According to the theory of planned behavior, subjective norms reflect expectations of relevant others and signal the valued social behavior to an individual. Prior studies on ISS policy compliance have shown that employees strive to maintain a positive image

by acting in accordance with the expectations of peers, superiors, and managers (Herath and Rao, 2009b; Yazdanmehr and Wang, 2016). Thus, this study considers subjective norms as social pressure which prevents an employee from engaging in NWRC. In addition to subjective norms, studies in social psychology have emphasized the role of descriptive norms in predicting behavior (Cialdini and Trost, 1998; Sheeran and Orbell, 1999). Sheeran and Orbell (1999) argue that descriptive and subjective norms are distinct forms of social influence, and that descriptive norms, the behavior of significant others, motivate an individual by informing them of typical or normal behaviors in a certain domain. They tested the theory of planned behavior, including descriptive norms and anticipated regret, and found that both constructs significantly influence the intention to participate in a lottery game. Therefore, this study conceptualized formal sanctions as punishment severity and detection certainty, and informal sanctions as subjective and descriptive norms. The following section introduces the hypotheses for this study.

In this study, punishment severity refers to employees' perception of the likelihood of being severely punished if caught using IT resources provided by the organization for non-work-related purposes (Li et al., 2010; Siponen and Vance, 2010). LLT suggests that the presence of a law enhances and shapes perceptions of the rightness and social acceptability of a certain behavior (Strelan and Boeckmann, 2006; Tyler and Darley, 2000). According to GDT, a high level of punishment increases the perceived risk of certain behavior and in turn decreases the occurrence of the law- and rule-abiding behaviors. Prior studies in IS field have found that punishment severity as a one characteristic of formal sanctions negatively influences IS-related deviant behavior (D'Arcy et al., 2009; Herath and Rao, 2009a; Li et al., 2010).

Therefore, this study argues that the relationship between punishment severity and NWRC will be mediated by an employee's moral beliefs against the behavior. In the NWRC context, when employees perceive a severe level of punishment for their behavior, they view the behavior as morally wrong and become less likely to engage in that behavior. In other words, punishment severity indirectly influences employees' NWRC through developing and/or strengthening employees' moral beliefs against NWRC. Thus, this study can present the following hypothesis:

H1: Punishment severity demotes NWRC intention because it increases moral beliefs. Specifically, the relationship between punishment severity and NWRC intention will be positively mediated by moral beliefs.

In this study, we have defined detection certainty as employees' perception of the probability that they will be caught if they use IT resources provided by the organization for non-work-related purposes (Li et al., 2010). High detection certainty increases the risk of being caught and penalized for the behavior. Prior studies have found that a low level of detection certainty is related to increased frequency of employee theft (Lau et al., 2003) and software piracy (Peace et al., 2003). Drawing on LLT, as a sub-dimension of formal sanctions, detection certainty has a positive impact on employee's moral beliefs which in turn deter NWRC. This study, hence, posits that detection certainty indirectly influences employees' NWRC through developing and/or strengthening employees' moral beliefs against NWRC. In other words, the higher the probability of being caught, the stronger the employees' beliefs against NWRC, which in turn, decreases NWRC. Thus, this study presents the following hypothesis:

H2: Detection certainty demotes NWRC intention because it increases moral beliefs. Specifically, the relationship between detection certainty and NWRC intention will be positively mediated by moral beliefs.

Subjective norms in our study refer to the employee's beliefs as to whether or not important others think the individual should engage in NWRC (Herath and Rao, 2009b; Peace et al., 2003). TPB posits that subjective norms are crucial factor which motivate behavior through the perception of gaining approval or disapproval from significant others for one's intentions and actions (Sheeran and Orbell, 1999). Inside organizations, employees are likely to avoid being disrespected by coworkers for unethical or inappropriate actions. Although they might not be reprimanded directly, leaving a bad impression could tarnish their reputation and positive image in the long term. On the other hand, as LLT suggests that the presence of a law enhances and shapes perceptions of the rightness and social acceptability of a certain behavior, subjective norms, which is unwritten rules inside organizations, can inform employees regarding the acceptable or unacceptable behaviors (Strelan and Boeckmann, 2006; Tyler and Darley, 2000). Thus it is reasonable to posit that the influence of subjective norms on NWRC will become stronger when employees internalize these norms as moral beliefs. Specifically, the more strongly that significant others think they should not to engage in NWRC results in stronger employees' beliefs against NWRC. For instance, Yazdanmehr and Wang (2016) provided empirical evidence that when employees perceive that IS policy compliance is what their supervisor or manager thinks they should do, they are more likely to internalize the compliance behavior as their personal norms, and in turn, comply with the policy. Given that employees are likely rational individuals

who strive to keep a positive image of themselves among peers and superiors at work, higher subjective norms result in stronger beliefs against NWRC and less likelihood that they engage in these behaviors. If an employee believes that important others disapprove of NWRC and will look down on them for these behaviors, they are less likely to engage in these behaviors. Therefore, this study posits the following hypothesis:

H3: Subjective norms demote NWRC intention because it increases moral beliefs. Specifically, the relationship between subjective norms and NWRC intention will be positively mediated by moral beliefs.

Descriptive norms refer to the extent to which one believes similar others are not performing NWRC (Herath and Rao, 2009b). In other words, descriptive norms represent the actual behavior of similar others within the organization. Sheeran and Orbell (1999) posited that the behavior of others motivates an individual by showing him or her what is the normal thing to do. Supported by law legitimacy theory, it is argued that the influence of descriptive norms on NWRC will become stronger when employees internalize norms as their moral beliefs. When employees believe that others are engaging in a behavior, they tend to also believe that the behavior is more appropriate within the organization. Thus, descriptive norms serve efficiency and accuracy functions, and the extent to which they affect behavior can indicate the extent to which a desire to be socially appropriate drives individuals (Cialdini and Trost, 1998). That is, the pervasiveness of NWRC could result in greater NWRC. Individuals could argue that because their coworkers act the behavior without any official censure, NWRC must be acceptable or harmless to the organization. The more pervasive

NWRC is among coworkers, the more likely it is that employees will engage in it. Employees are likely to imitate their coworkers' behavior. In other words, lesser amounts of significant others that engage in NWRC result in stronger employees' beliefs against NWRC, which in turn decreases NWRC. Therefore, this study posits the following hypothesis:

H4: Descriptive norms demote NWRC intention because it increases moral beliefs. Specifically, the relationship between descriptive norms and NWRC intention will be positively mediated by moral beliefs.

3.3. Construct Measurement

All measurement items were adapted from prior studies and modified to fit the context of NWRC. NWRC intention was operationalized by capturing the likelihood of engaging in NWRC and measured with five items adapted from Chatterjee et al. (2015). Punishment severity (PS) refers to the extent to which an employee perceives punishment to be severe, and three items from Siponen and Vance (2010) gauged the severity of punishment. Detection certainty (DC) was measured with three items modified from the scale of Siponen and Vance (2010) and captured the possibility of detection. Items regarding subjective norms (SN) were adapted from Moody et al. (2018). Descriptive norms (DN) were measured with four items adapted from Yazdanmehr and Wang (2016). The measurement items were designed to capture employees' perception of coworkers' behavior. Moral beliefs (MB) were operationalized by capturing the employee's judgment regarding NWRC intention and measured with three items from Li et al. (2010) and Xu et al. (2016). All items were measured on a seven-point Likert scale, ranging from one (strongly disagree) to seven (strongly agree). As the target

<Table 2> Sources of Measurement Items

Construct	Operational definition	Sources of items
NWRC intention	The extent to which an employee is apt to engage in NWRC	Chatterjee et al. (2015)
Punishment severity	The extent to which an employee perceives punishment to be severe	Siponen and Vance (2010)
Detection certainty	The extent to which an employee perceives his/her act to be caught	Siponen and Vance (2010)
Subjective norms	The extent to which an employee believes whether or not the important others inside the organization think the individual not to engage in NWRC (expectations of relevant others)	Moody et al. (2018)
Descriptive norms	The extent to which an employee believes coworkers are not performing NWRC (behavior of similar others)	Yazdanmehr and Wang (2016)
Moral beliefs	The extent to which an employee evaluates the NWRC as morally wrong	Li et al. (2010), Xu et al. (2016)

sample included employees in Mongolia, and the original measures of the studied constructs were developed in English, the survey instrument was translated from English into Mongolian. After the translation, the English language center teacher was asked to ensure whether the Mongolian version was equivalent to the original English questionnaire. <Table 2> shows the operational definitions of constructs and sources of items for each construct.

IV. Data Analysis

4.1. Research Approach and Data Collection

IS security research typically begins with a hypothetical scenario which is meant to “trigger” a person’s decision-making process regarding behaviors. In line with prior research, this study used a scenario-based survey instrument to test the research model and hypotheses. The first step of our survey was designed to capture NWRC using a scenario approach which involved examples of employees’ NWRC and disciplinary actions resulted from these behaviors. For the sake of clarity, the survey included a definition for NWRC. In the next step, we administrated a

survey that targeted employees who assumed the situation described in the scenario.

We have also considered the banks as the target samples because employees in the banks often use information systems in their offices in comparison to other industries. For data collection, employees working in headquarters of banks in Mongolia responded to paper-based questionnaires from the end of March to the beginning of April 2018. Questionnaires were distributed to human resources managers in all banks in Mongolila and data was collected from seven banks. No rewards were provided to each survey recipient after suvery completion. In total, 223 completed surveys were collected. Due to incomplete 47 incomplete responses, a total of 176 cases were retained for further analysis.

4.2. Research Methodology

In this study, we chose PLS to test both measurement model and structural model because it places minimal restrictions on sample size and allows for the examination of all paths in the model simultaneously (Chin, 1998). We also adopted two types of regression analysis (Baron and Kenny, 1986;

Hayers, 2013) by using SPSS 20 in order to drill down deeper on the mediation implied by the PLS analysis as well as to show no threats of common method bias by employing different techniques.

To test the measurement model, convergent validity and discriminant validity were assessed (Hair et al., 2009). Regarding convergent validity, individual item reliability and construct reliability were tested through the item-to-construct loadings, the composite reliability (CR), Cronbach's α and the average variance extracted (AVE). Discriminant validity was tested by calculating cross-loadings indicators and comparison of the square root of AVE with correlation values among constructs. The structural model was assessed using PLS analysis, followed by *post-hoc* regression analyses to find a consistent pattern of mediating effect on the moral beliefs in the study.

4.3. Sample Profiles

<Table 3> shows the demographic characteristics of the study sample. As depicted in the table, the sample included 62 (35.2%) males and 114 (64.8%) females. Most respondents were aged 20-39 ($M = 30.70$, $SD = 5.37$). Type of employment was measured

in terms of full- and part-time, as well as workplace and home, and the majority of respondents were full-time employees working at workplaces.

4.4. Measurement Model

In our measurement model, the psychometric properties of scales were examined in terms of convergent validity and discriminant validity. Our results found that the lowest item loading was 0.747, which demonstrates adequate convergent validity as represented in <Appendix B>. On the basis of factor analysis, six items which exhibited loadings lower than 0.70 were dropped (In <Appendix A>, marked with *). Next, we calculated CR, Cronbach's α , and AVE for the reliability. As shown in <Table 4>, all constructs in the measurement model exceeded the recommended threshold values and exhibited CR of 0.917 or higher, Cronbach's α of 0.863 or higher, and AVE of 0.761 or higher (Hair et al., 2009).

Discriminant validity was examined by comparing the square root of the AVE for each construct with bivariate correlations between that and all other constructs. As indicated in <Table 5>, the square root of AVE values for each construct is higher than

<Table 3> Sample Demographics

Variable	Category	Frequency	Percentage (%)
Gender	Male	62	35.2
	Female	114	64.8
Age	20 to 29 years	78	44.3
	30 to 39 years	85	48.3
	40 to 49 years	12	6.8
	Above 50 years	1	0.6
Type of employment	Full time position work from office	174	98.8
	Full time position work from home several times a week	2	1.2
	Part time position work from office	-	-
	Part time position work from home several times a week	-	-

<Table 4> Descriptive Statistics and Reliability of Constructs

Constructs	Mean	SD	Cronbach's <i>a</i>	CR	AVE
NWRC	3.276	1.509	0.926	0.945	0.776
PS	4.244	1.560	0.873	0.921	0.796
DC	4.706	1.459	0.898	0.936	0.829
SN	4.926	1.411	0.895	0.927	0.761
DN	4.085	1.524	0.948	0.962	0.864
MB	4.354	1.435	0.863	0.917	0.786

Note: NWRC, non-work-related computing intention; PS, punishment severity; DC, detection certainty; SN, subjective norms; DN, descriptive norms; MB, moral beliefs; SD, standard deviation; CR, composite reliability; AVE, average variance extracted

<Table 5> Correlations Among Constructs and Assessment of Discriminant Validity

Constructs	NWRC	PS	DC	SN	DN	MB
NWRC	0.881					
PS	-0.135	0.892				
DC	-0.148	0.420	0.910			
SN	-0.194	0.388	0.562	0.872		
DN	-0.384	0.182	0.401	0.431	0.930	
MB	-0.387	0.324	0.462	0.477	0.553	0.886

Note: NWRC, non-work-related computing intention; PS, punishment severity; DC, detection certainty; SN, subjective norms; DN, descriptive norms; MB, moral beliefs.

The bold values in the main diagonal are the square root of AVE value for the corresponding constructs.

the highest bivariate correlation between any construct pair, which shows a satisfactory level of discriminant validity (i.e., the lowest value for the square root of AVE is 0.872, and the highest correlation value between construct pairs is 0.562).

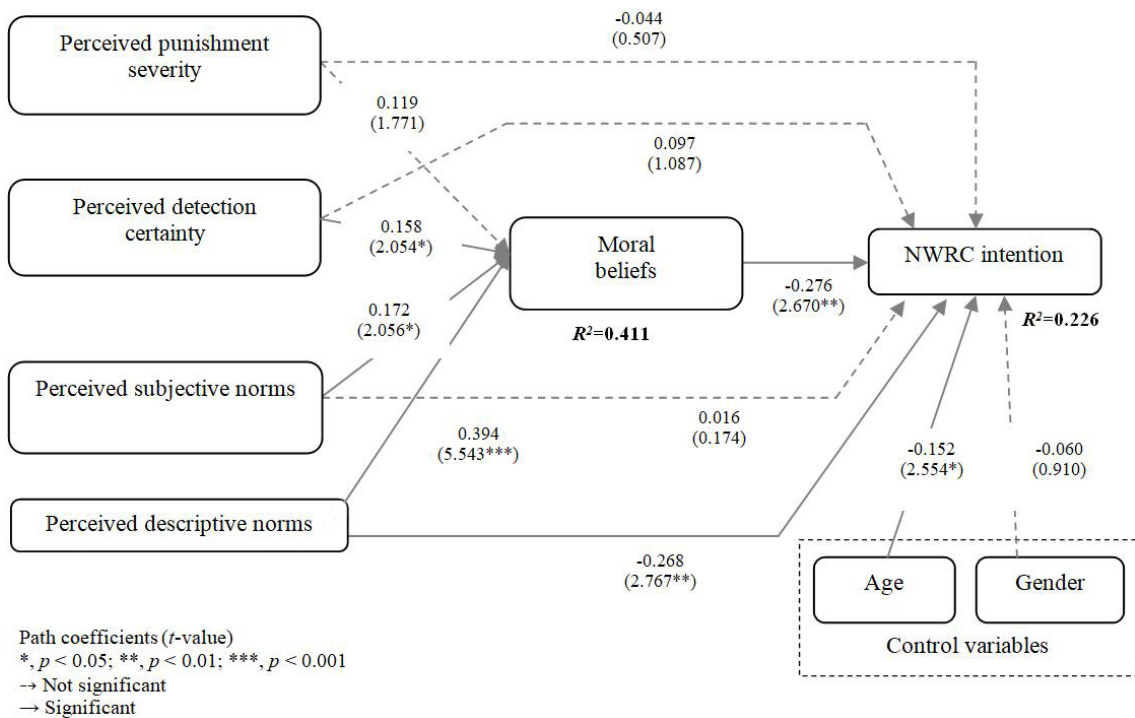
Common method bias was analyzed as shown in <Appendix C>, since all construct measures in the model were collected at the same time using the same data collection method. The results suggested that this bias is not present in this study.

4.5. Hypothesis Testing

In this study, we conducted two different approaches to test the mediation. We began by examining the structural model using PLS analysis. To obtain

a detailed understanding of the mediation of moral beliefs, we followed up with two regression analysis-based approach such as Baron and Kenny (1986)'s and Hayes (2013)'s ones. In PLS analysis, the algorithm and the bootstrapping re-sampling method using 176 cases and 5000 bootstrapping samples were conducted to estimate the structural model, as suggested by Chin et al. (2003). <Figure 2> shows our results of PLS analysis.

As shown in <Figure 2>, 22.6 percent of the variance was explained for NWRC intention. The R^2 value for the mediating variable, moral beliefs, was 0.411 (41.1%). As shown in <Figure 2>, the path between DC and MB ($\beta = 0.158, t = 2.054$); the path between SN and MB ($\beta = 0.172, t = 2.056$); the path between DN and MB ($\beta = 0.394, t = 5.543$);



<Figure 2> Analysis of Mediation Effect Using PLS Analysis

and the path between MB and NWRC intention ($\beta = -0.276$, $t = 2.670$) were all significant, suggesting that the MB mediates the relationships between independent variables and the dependent variable. The direct path between DN and NWRC intention was found to be significant ($\beta = -0.268$, $t = 2.767$), suggesting partial mediation. In addition, age, which was one of control variables, significantly influenced NWRC intention ($\beta = -0.152$, $t = 2.054$, $p < 0.05$), which implies that people are less likely to engage in NWRC intention as they age.

We further conducted two different mediated regression analyses such as Baron and Kenny (1986) and Hayes (2013) approaches to re-test the mediating effect of moral beliefs on NWRC intention. The results of the mediation analysis are presented in <Table 6> and <Table 7>. According to the results from the Baron and Kenny (1986)'s approach, while moral

beliefs fully mediate the effects of detection certainty and subjective norms on NWRC intention, it partially mediates the effect of descriptive norms on NWRC intention. Sobel test statistics are significant for DC, SN, and DN, indicating that these factors have a significant indirect effect on NWRC intention and mediated by moral beliefs.

Next, in Hayes (2013)'s approach, we adopted Preacher and Hayes's procedures with a bootstrap resampling size of 5000 to calculate the significance of indirect effects. Using macro for SPSS and bootstrapping method, the indirect effect was tested and results are presented in <Table 7>.

<Table 8> provides a summary of the results for all of the hypotheses that were tested. As shown in <Table 8>, all of our hypotheses were supported, with exception of H1.

<Table 6> Mediation Test Results Following the Baron and Kenny (1986) Approach

#	Steps	Coefficients	R ²
1	IV → Mediator (PS, DC, SN, DN → MB)	PS = 0.121 (t = 1.825) DC = 0.154 [†] (t = 2.050) SN = 0.166 [†] (t = 2.217) DN = 0.400 ^{***} (t = 6.035)	0.393
2	IV → DV (PS, DC, SN, DN → NWRC)	PS = -0.071 (t = -0.896) DC = 0.058 (t = 0.646) SN = -0.031 (t = -0.344) DN = -0.382 ^{***} (t = -4.822)	0.134
3	IV and Mediator → DV (PS, DC, SN, DN, MB → NWRC)	PS = -0.038 (t = -0.482) DC = 0.101 (t = 1.133) SN = 0.015 (t = 0.169) DN = -0.272 ^{***} (t = -3.192) MB = -0.276 ^{***} (t = -3.090)	0.175
4	Sobel test $Z \text{ value} = a * b / \sqrt{(b^2 * s_a^2 + a^2 * s_b^2)}$	Z = -4.091 ^{***} (p < 0.001) (DC → MB → NWRC) Z = -3.968 ^{***} (p < 0.001) (SN → MB → NWRC) Z = -2.864 ^{**} (p = 0.004) (DN → MB → NWRC)	

Note: [†]p < 0.05; ^{**}p < 0.01; ^{***}p < 0.001

IV, independent variable; PS, punishment severity; DC, detection certainty; SN, subjective norms; DN, descriptive norms; MB, moral beliefs; DV, dependent variable; NWRC, non-work-related computing intention

<Table 7> Mediation Test Results Following the Hayes (2013) Approach

Effects of IVs (PS, DC, SN, DN) on DV (NWRC intention)						
	Direct effect			Total effect		
	Estimate	S.E.	t value	Estimate	SE.	t value
PS	-0.025	0.072	-0.036	-0.121	0.073	-1.659
DC	0.047	0.081	0.579	-0.143	0.078	-1.847
SN	-0.008	0.085	-0.089	-0.197	0.080	-2.476 [*]
DN	-0.245	0.081	-3.023 ^{**}	-0.381	0.069	-5.494 ^{***}
Indirect effect (bootstrap)		Estimate	LLCI	ULCI	Mediation supported?	
PS → MB → NWRC		-0.118	-0.201	-0.054	No mediation	
DC → MB → NWRC		-0.191	-0.303	-0.098	Full mediation	
SN → MB → NWRC		-0.190	-0.306	-0.092	Full mediation	
DN → MB → NWRC		-0.135	-0.242	-0.040	Partial mediation	

Note: ^{*}p < .05; ^{**}p < .01; ^{***}p < .001

IV, independent variables; PS, punishment severity; DC, detection certainty; SN, subjective norms; DN, descriptive norms; MB, moral beliefs; DV, dependent variable; NWRC, non-work-related computing intention

<Table 8> Summary of Hypotheses Testing Results

#	Hypotheses	Results
H1	Punishment severity demotes NWRC intention because it increases moral beliefs. Specifically, the relationship between punishment severity and NWRC intention will be positively mediated by moral beliefs.	Not supported
H2	Detection certainty demotes NWRC intention because it increases moral beliefs. Specifically, the relationship between detection certainty and NWRC intention will be positively mediated by moral beliefs.	Supported
H3	Subjective norms demote NWRC intention because it increases moral beliefs. Specifically, the relationship between subjective norms and NWRC intention will be positively mediated by moral beliefs.	Supported
H4	Descriptive norms demote NWRC intention because it increases moral beliefs. Specifically, the relationship between descriptive norms and NWRC intention will be positively mediated by moral beliefs.	Supported

4.6. Discussion

First, this study investigated how employee perception of punishment severity enhances their moral beliefs against NWRC intention, and in turn, deters the behavior. According to our results, perceived punishment severity may not directly or indirectly impede employees' NWRC intention. However, prior research in the IS security field has indicated different results regarding this relationship. Li et al. (2014), Li et al. (2010) found that sanction severity has an insignificant effect on Internet policy compliance intention while D'Arcy et al. (2009) demonstrated that severity of sanctions could deter information systems misuse intention. Interestingly, in Herath and Rao (2009b) and Chen et al. (2012), severity of punishment decreases the intention to comply with policies. These studies interpreted the insignificant results as (1) employees may perceive the punishment resulting from NWRC intention as not severe enough to view this behavior as inappropriate; (2) the perception of punishment severity is higher if coworkers who engage in NWRC intention have not been punished for their actions, and employees might feel the behavior is not morally wrong. However, considering the inconsistent findings of punishment severity, there might be little effect of punishment severity on IS misuse intention, including NWRC intention. In this study context, the path coefficient punishment severity on moral beliefs was 0.119 ($t = 1.771$). Moreover, our results from Hayes (2013)'s approach, punishment severity had a significant indirect effect on NWRC via moral beliefs ($b = -0.118$, with a 95% CI of -0.201 to -0.054), indicating that moral beliefs fully mediate the impact of punishment severity on NWRC intention. This inconsistent result might be derived from the small sample size of 176 employees. Thus, future research should consider the issue of

sample size effects to examine the effect of punishment severity on moral beliefs, which deter NWRC intention.

Second, our results found that the greater the perceived detection certainty results in the more likely employees are to view this behavior as morally unacceptable. Specifically, detection certainty enhances employee perception that the behavior is morally wrong. Our results showed that detection certainty has no direct effect on NWRC intention, although prior research found a significant negative relationship. The actual punishment level for the behavior can explain the insignificant direct effect. Even though there are policies and procedures which posit employees engaged in NWRC intention would be easily detected and severely punished, these appear inadequate to deter employees. Compared to punishment severity, detection certainty may be more visible and understandable to employees, and being detected does not mean s/he will be punished. Thus, detection certainty may significantly strengthen employees' moral beliefs against NWRC intention. This result has been consistent with D'Arcy and Devaraj (2012) such that certainty of formal sanction enhances moral beliefs, and in turn, deters the misuse of IT resources.

Third, unlike formal sanctions (i.e., punishment severity and detection certainty), informal sanctions seem to have stronger impacts on moral beliefs. Subjective norms, which refer to the expectations of managers and coworkers, significantly shape employees' moral beliefs and deter NWRC intention. Being disrespected by managers and coworkers for unethical or inappropriate actions provide employees information regarding the rightness of the act.

Finally, this study investigated how descriptive norms deter employees' NWRC intention directly and indirectly. Results illustrated that descriptive norms have a stronger significant influence on

NWRC and moral beliefs. To a greater extent, it seems that actual behaviors in the surrounding environment exert strong effects on moral beliefs and employees' likelihood to engage in such behaviors. As mentioned prior, the pervasiveness of deviant behaviors result in greater amounts of deviant behaviors. Conversely, less incidence of behaviors inside organizations result in greater occurrence of employees viewing the behavior as wrong and inappropriate. Employees are likely to imitate coworkers' behavior consciously as well as automatically.

Overall, results suggest that moral beliefs concerning behaviors are a good predictor of NWRC intention - that is, employees have NWRC intention as morally wrong are less apt to engage in such behaviors. This finding is consistent with the perspective of law legitimacy theory, which posits that external factors enhance the perception that illicit behavior is morally wrong.

V. Conclusion

5.1. Research Summary

This study has developed a moral-beliefs based model by integrating constructs derived from law legitimacy theory, general deterrence theory, and planned behavior theory. More specifically, we have examined the mediating effect of moral beliefs on the relationships between sanctions (i.e., formal and informal sanctions) and NWRC intention. This study has considered both punishment severity and detection certainty as formal sanctions, while subjective and descriptive norms were regarded as informal sanctions. Based upon the literature review, we posited four mediated hypotheses and collected 176 data from employees working in Mongolian banks to test

the research hypotheses. PLS was employed to test both measurement and structural models with a two different types of mediated regression analyses for examining the consistent pattern the effects of moral beliefs. All hypotheses were statistically significant except for Hypothesis 1. We found that moral beliefs could act as a full mediator in the relationships between detection certainty/subjective norms and NWRC intention. We also found that moral beliefs act as a partial mediator in the relationship between descriptive norms and NWRC intention.

5.2. Implications for Research and Practice

This study makes several research contributions to the NWRC literature.

First, our main contribution is that it develops and tests a theoretically grounded model of NWRC by employing moral beliefs. For building the research model, key constructs from several theories in different research area such as criminology (i.e., law legitimacy theory), psychology (i.e., general deterrence theory), IS field (i.e., theory of planned behavior) were intergeated into a single framework to develop theoretical mechanisms of deterring NWRC. We assure that it offers novel theoretical explanations, based on several theories, for how NWRC is reduced in organizations.

Second, this study contributes to the discourse pertaining individuals' judgement and behavior literature by developing the moral beliefs. The moral beliefs has been related to an individuals' judgement of right or wrong about a specific behavior. While it was well-defined in numerous research areas, the relevant literature is devoid of research that investigates theoretically position of the moral beliefs. In this study, we provide empirical evidences that moral beliefs could be a mediator in the relationships be-

tween formal/informal sanctions and NWRC intention by conducting several different types of analyses. By providing those evidences that the moral beliefs could control employees' NWRC, we contribute to relevant work for exploring the deterrence of NWRC.

Third, this study has classified two major drivers for controlling the effect of NWRC such as formal and informal sanctions by systematically reviewing criminology and psychology literature. In our review, we have considered both punishment severity and detection certainty as formal sanctions, while subjective norms and descriptive norms as informal sanctions as major drivers of deterring employees' NWRC. Even though each construct has been explored in different research areas, our classifications allowed relevant research to generate insights into one possible mechanism underlying employees' NWRC, by focusing our attention on both formal sanctions (i.e., punishment severity and detection certainty) and informal sanctions (i.e., subjective norms and descriptive norms) of controlling the NWRC intention.

This study also makes several practical implications.

First, our findings emphasized that practitioners should focus on employees' moral beliefs in order to control NWRC. Since employees who judge NWRC as a wrong act are less likely to engage in NWRC, it is necessary to develop their moral beliefs against these behaviors. Stronger moral beliefs against NWRC can voluntarily regulate employees engaging in NWRC in the long run. In order to strengthen employees' moral beliefs, organizations need to institute effective policies and promote a culture opposing NWRC by educating employees about the negative consequences of NWRC for both their productivity and the organization's IS security. For example, it might be effective to introduce organizational principles regarding NWRC to new employees from

the first day of their employment.

Second, this study has introduced that well-established formal sanctions (e.g., severe punishment and detection certainty) may emerge as a means to develop employees' moral beliefs. The purpose of formal sanctions is to increase employees' perceived risks or costs of engaging in NWRC. Therefore, it is suggested that instituting policy which prohibits NWRC will be an effective measure for employers to provide employees direction about whether it is right to engage in NWRC. More specifically, the disciplinary actions for NWRC should be fitted to the type and magnitude of the behavior; and the occurrence of the behavior should be detected and punished in real-time.

Finally, in our findings, informal sanctions play a significant role in enhancing moral beliefs and deterring NWRC. To increase informal sanctions within organizations, creating an IS security culture is one of the more influential means. Organizations can create such their own culture by: (1) making employees aware that NWRC is not an expectation of managers with the inclusion of IS security duties in every job description, and (2) by allowing brief periodic NWRC to encourage employees to use it both as a recovery tool during working hours and as a means for managing life needs.

5.3. Limitations and Future Research

While this study contributes to both research and practice, there are limitations that can be addressed in future research. First, the characteristics of respondents, especially the majority of the younger employees in the sample may limit the generalizability of findings. Considering the theoretical foundations and prior research, however, the findings provide valid contributions to the literature on NWRC.

Secondly, recent studies have categorized employees' non-work-related computing in terms of its continuance (i.e., short time vs. long time) (Kuem and Siponen, 2014), cognitive efforts (i.e., high cognitive efforts vs. low cognitive efforts) (Lim and Chen, 2012) or underlying motives (i.e., expressive vs. instrumental) (Willison and Warkentin, 2013). Future research needs to examine the relationship between moral beliefs and the mentioned constructs in the NWRC context. Finally, while we have adopted cross-sectional survey approach to capture the relationship

between sanctions and NWRC by mediating the moral beliefs, it is necessary to see the dynamics of NWRC (e.g., how does employees' NWRC occur, detect and reduce) in organizations. For this, it might be appropriate to conduct a longitudinal approach.

Acknowledgement

This research was based on the thesis of Master Tserendulam Munkh-Erdene.

<References>

- [1] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- [2] Bachman, R., Paternoster, R., and Ward, S. (1992). The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law and Society Review*, 26(2), 343-372.
- [3] Baron, R. M., and Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 51(6), 1173-1182.
- [4] Bock, G. W., and Ho, S. L. (2009). Non-work related computing (NWRC). *Communications of the ACM*, 52(4), 124-128.
- [5] Chatterjee, S., Sarker, S., and Valacich, J. S. (2015). The behavioral roots of information systems security. *Journal of Management Information Systems*, 31(4), 49-87.
- [6] Chen, Y., Ramamurthy, K., and Wen, K.-W. (2012). Organizations' information security policy compliance: stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157-188.
- [7] Cheng, L., Li, W., Zhai, Q., and Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, 38, 220-228.
- [8] Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security*, 39(PART B), 447-459.
- [9] Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295(2), 295-336.
- [10] Chin, W. W., Marcolin, B. L., and Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, 14(2), 189-217.
- [11] Cialdini, R. B., and Trost, M. R. (1998). Social influence: Social norms, conformity and compliance. In and G. L. D. T. Gilbert, S. T. Fiske (Ed.), *The handbook of social psychology* (pp. 151-192). New York, NY, US: McGraw-Hill.
- [12] Cohen, J. (1992). Statistical power analysis. *Current Directions in Psychological Science*, 1(3), 98-101.
- [13] D'Arcy, J., and Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, 43(6), 1091-1124.
- [14] D'Arcy, J., and 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.
- [15] D'Arcy, J., Hovav, A., and 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.
- [16] D'Arcy, J., and Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 1-27.
- [17] Everton, W. J., Mastrangelo, P. M., and Jolton, J. A. (2005). Personality correlates of employees' personal use of work computers. *CyberPsychology and Behavior*, 8(2), 143-153.
- [18] Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York, NY, US: Elsevier.
- [19] Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203-236.
- [20] Hair, J. J., Black, W. C., Babin, B. J., and Anderson, R. E. (2009). *Multivariate data analysis* (7th ed.). Englewood Cliffs: Prentice Hall.
- [21] Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: a regression based approach* (1st ed.). New York, NY, US: The Guilford Press.
- [22] Herath, T., and Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.
- [23] Herath, T., and Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(August 2008), 106-125.
- [24] Hu, Q., Xu, Z., Dinev, T., and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6), 54.
- [25] Hunt, S. D., and Vitell, S. (1986). A general theory of marketing ethics. *Journal of Macromarketing*, 6(1), 5-16.
- [26] Khansa, L., Kuem, J., Siponen, M., and Kim, S. S. (2017). To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems*, 34(1), 141-176.
- [27] Kim, S. J., and Byrne, S. (2011). Conceptualizing personal web usage in work contexts: A preliminary framework. *Computers in Human Behavior*, 27(6), 2271-2283.
- [28] Kuem, J., and Siponen, M. (2014). Short-time non-work-related computing and creative performance. In *47th Hawaii International Conference on System Sciences (HICSS)* (pp. 3215-3223).
- [29] Lau, V. C., Au, W. T., and Ho, J. M. (2003). A qualitative and quantitative review of antecedents of counterproductive behavior in organizations. *Journal of Business and Psychology*, 18(1), 73-99.
- [30] Li, H., Sarathy, R., Zhang, J., and Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, 24(6), 479-502. <https://doi.org/10.1111/isj.12037>
- [31] Li, H., Zhang, J., and Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), 635-645.
- [32] Liang, H., Saraf, N., Hu, Q., and Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, 31(1), 59-87.
- [33] Lim, V. K. G. (2005). The moderating effect of neutralization technique on organizational justice and cyberloafing. In *PACIS2005*.
- [34] Lim, V. K. G., and Chen, D. J. Q. (2012). Cyberloafing at the workplace: Gain or drain on work? *Behaviour and Information Technology*, 31(4), 343-353.

- [35] Lindell, M. K., and Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research design. *Journal of Applied Psychology*, 86(1), 114-121.
- [36] Magnuson, M. J., and Dundes, L. (2008). Gender differences in "social portraits" reflected in MySpace profiles. *CyberPsychology and Behavior*, 11(2), 239-241.
- [37] Malhotra, N. K., Kim, S. S., and Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, 52(12), 1865-1883.
- [38] Moody, G. D., Siponen, M., and Pahlila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 285-311.
- [39] Moores, T. T., and Chang, J. C. J. (2006). Ethical decision making in software piracy: Initial development and test of a four-component model. *MIS Quarterly*, 30(1), 167-180.
- [40] Nagin, D. S., and Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, 39(4), 865-892.
- [41] Paternoster, R., and Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, 30(3), 549-583.
- [42] Peace, A. G., Dennis, F. G., and Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*, 20(1), 153-177.
- [43] Pee, L. G., Woon, I. M. Y., and Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information and Management*, 45(2), 120-130.
- [44] Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.
- [45] Schoepfer, A., and Piquero, A. R. (2006). Self-control, moral beliefs, and criminal activity. *Deviant Behavior*, 27(1), 51-71.
- [46] Sheeran, P., and Orbell, S. (1999). Augmenting the theory of planned behavior: Roles for anticipated regret and descriptive norms. *Journal of Applied Social Psychology*, 29(10), 2107-2142.
- [47] Siponen, M., and Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502.
- [48] Statista. (2015). *Increased risk of cyber breach or insider threat according to executives worldwide as of September 2015, by industry*. Retrieved from <https://www.statista.com/statistics/594093/risk-of-cyber-breach-misuse-by-industry/>
- [49] Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276.
- [50] Strelan, P., and Boeckmann, R. J. (2006). Why drug testing in elite sport does not work: Perceptual deterrence theory and the role of personal moral beliefs. *Journal of Applied Social Psychology*, 36(12), 2909-2934.
- [51] Thong, J. Y., and Yap, C. S. (1998). Testing an ethical decision-making theory: The case of soft lifting. *Journal of Management Information Systems*, 15(1), 213-237.
- [52] Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annual Review of Psychology*. <https://doi.org/10.1146/annurev.psych.57.102904.190038>
- [53] Tyler, T. R., and Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, 48(6), 1143-1158.
- [54] Tyler, T. R., and Darley, J. M. (2000). Building a law-abiding society: Taking public views about morality and the legitimacy of legal authorities into account when formulating substantive law. *Hofstra Law Review*, 28, 707-739.
- [55] Vitak, J., Crouse, J., and LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, 27(5), 1751-1759.

- [56] Willison, R., and Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1), 1-20.
- [57] World Economic Forum. (2018). *The global risks report 2018*, 13th edition. Cologny/Geneva Switzerland. <https://doi.org/978-1-944835-15-6>
- [58] Xu, B., Xu, Z., and Li, D. (2016). Internet aggression in online communities: a contemporary deterrence perspective. *Information Systems Journal*, 26(6), 641-667.
- [59] Yazdanmehr, A., and Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 92, 36-46.

<Appendix A> Measurement Items

Scenario: You are an employee in Venple Co., which is one of the most IT-driven service companies in your country. According to company's IT use policy, you have already recognized that employees are not allowed to engage in NWRC activities and use ICT resources irrespective of their access level. Your company closely keeps track of your IT use (e.g., Internet, emails, SNS, online news, software downloads, and financial transactions) within its physical and virtual confines. It also results in disciplinary actions up to and including termination of employment. However, you might access the Internet during the work hours if you want. To save your time and effort in your daily life, you could check your personal emails, use your SNS to maintain interpersonal relationships, make a reservation on concert, and make a purchase in online shopping for your private needs in your company.

Constructs	Items		Sources
Non-work-related computing intention (NWRC)	NWRC1	If I were to carry out NWRC, it makes sense for me to do it.*	Chatterjee et al. (2015)
	NWRC2	Depending on the situation, I could carry out NWRC.	
	NWRC3	If I had the opportunity, I would carry out NWRC.	
	NWRC4	All things considered, it is likely that I might carry out NWRC in the future.	
	NWRC5	All things considered, I expect to carry out NWRC in the future.	
	NWRC6	I intend to carry out NWRC in the future.	
Punishment severity (PS)	PS1	My company disciplines employees who engaged in NWRC.*	Siponen and Vance (2010)
	PS2	My company terminates employees who repeatedly engage in NWRC.*	
	PS3	It would be a great problem if I received severe sanctions when I engaged in NWRC.	
	PS4	It would create a great problem in my life if I were formally sanctioned for engaging in NWRC.	
	PS5	It would create a great problem in my life if I were formally reprimanded for engaging in NWRC.	
Detection certainty (DC)	DC1	If I do engage in NWRC, I would probably be caught.*	Siponen and Vance (2010)
	DC2	Employee computer practices are properly monitored for engaging in NWRC.*	
	DC3	I would receive corporate sanctions if I engage in NWRC.	
	DC4	I would be formally sanctioned if management learned that I had engaged in NWRC.	
	DC5	I would be formally reprimanded if management learned I had engaged in NWRC.	
Subjective norms (SN)	SN1	Top management in my organization thinks I should not engage in NWRC.	Moody et al. (2018)
	SN2	My immediate supervisor in my organization thinks I should not engage in NWRC.	
	SN3	My coworkers think I should not engage in NWRC.	
	SN4	The security staff in my organization thinks I should not engage in NWRC.	
Descriptive norms (DN)	DN1	I believe other employees do not engage in NWRC.	Yazdanmehr and Wang (2016)
	DN2	I think most employees in my organization do not engage in NWRC.	
	DN3	I am convinced my coworkers do not engage in NWRC.	
	DN4	It is likely that the majority of other employees in my organization do not engage in NWRC.	
Moral beliefs (MB)	MB1	I think I should not engage in NWRC.	Li et al. (2010) Xu et al. (2016)
	MB2	To me, it is not acceptable to engage in NWRC.	
	MB3	To me, engaging in NWRC is a trivial offence.*	
	MB4	I would consider engaging in NWRC is morally wrong.	

Note: *Dropped to improve reliability or construct validity.

<Appendix B> Item-Factor Loading and Cross-Loading

Constructs	Items	NWRC	PS	DC	SN	DN	MB
Non-work-related computing intention	NWRC2	0.747	-0.021	-0.116	-0.123	-0.356	-0.291
	NWRC3	0.887	-0.143	-0.103	-0.125	-0.320	-0.295
	NWRC4	0.938	-0.157	-0.112	-0.170	-0.341	-0.368
	NWRC5	0.942	-0.130	-0.160	-0.213	-0.342	-0.379
	NWRC6	0.878	-0.139	-0.158	-0.217	-0.330	-0.361
Punishment severity	PS3	-0.153	0.849	0.391	0.324	0.158	0.270
	PS4	-0.154	0.939	0.383	0.389	0.209	0.338
	PS5	-0.025	0.887	0.342	0.311	0.094	0.238
Detection certainty	DC3	-0.212	0.416	0.919	0.506	0.425	0.472
	DC4	-0.111	0.344	0.923	0.543	0.359	0.405
	DC5	-0.054	0.380	0.889	0.487	0.290	0.369
Subjective norms	SN1	-0.135	0.374	0.525	0.896	0.334	0.421
	SN2	-0.125	0.388	0.505	0.902	0.317	0.398
	SN3	-0.250	0.270	0.470	0.807	0.506	0.467
	SN4	-0.142	0.330	0.449	0.882	0.301	0.347
Descriptive norms	DN1	-0.375	0.182	0.355	0.383	0.905	0.499
	DN2	-0.321	0.165	0.339	0.390	0.934	0.503
	DN3	-0.343	0.161	0.397	0.409	0.935	0.519
	DN4	-0.384	0.168	0.397	0.420	0.944	0.534
Moral beliefs	MB1	-0.370	0.258	0.457	0.453	0.540	0.916
	MB2	-0.328	0.334	0.371	0.445	0.467	0.905
	MB4	-0.329	0.272	0.397	0.366	.459	0.836

<Appendix C> Common Method Bias Testing

Three methods were used to assess common-method bias (CMB) (Podsakoff et al., 2003). The first method was Harman’s one-factor test, which is the simplest and most common statistical remedy to address CMB by entering all items into an unrotated exploratory factor analysis. As a result, six factors were present and most covariance was explained by one factor (37.45 percent), showing that CMB was not an issue for this study. Second, following Liang et al. (2007), a common method factor was added to the model and was allowed to be associated reflectively with items of all constructs. As shown in <Table C.1>, results demonstrate that the average substantive explained variance was 0.728, while the average method-based variance was 0.010. Moreover, the method factor loadings were not significant, suggesting that CMB had no significant impact on the sample data. Lastly, CMB was assessed using the marker variable method described by Lindell and Whitney (2001). Following the study of Malhotra et al.(2006), a marker variable which had the lowest correlation with study constructs was identified. In this method, CMB is assessed on the correlation between the marker variable and theoretically unrelated variables. The correlation was denoted by R_{MI} . Organizational commitment, which refers to the extent to which employees want to continue their organizational membership, was selected as a marker variable. It was measured with six items adapted from Posey, Roberts, and Lowry (2016). As shown in <Table C.2>, correlations between variables were decreased by a maximum of 0.024, with all insignificant correlations remaining insignificant and significant correlations remaining significant. Overall, the results of the CMB analyses suggest that CMB, if any is present, is not a significant factor in this study.

<Table C.1> Common Method Bias Analysis Using Common Method Factor

Constructs	Indicators	Substantive factor loading (R1)	R1 ²	Method factor loading (R2)	R2 ²
Non-work-related computing intention	NWRC2	0.638	0.407	0.095	0.009
	NWRC3	0.837	0.701	0.095	0.009
	NWRC4	0.924	0.854	0.100	0.010
	NWRC5	0.947	0.897	0.097	0.009
	NWRC6	0.866	0.750	0.096	0.009
Punishment severity	PS3	0.690	0.476	0.090	0.008
	PS4	0.948	0.899	0.096	0.009
	PS5	0.859	0.738	0.100	0.010
Detection certainty	DC3	0.838	0.702	0.104	0.011
	DC4	0.897	0.805	0.101	0.010
	DC5	0.839	0.704	0.107	0.011
Subjective norms	SN1	0.919	0.845	0.102	0.010
	SN2	0.919	0.845	0.107	0.011
	SN3	0.622	0.387	0.105	0.011
	SN4	0.814	0.663	0.098	0.010
Descriptive norms	DN1	0.845	0.714	0.099	0.010
	DN2	0.895	0.801	0.104	0.011
	DN3	0.919	0.845	0.101	0.010
	DN4	0.934	0.872	0.102	0.010
Moral beliefs	MB1	0.894	0.799	0.103	0.011
	MB2	0.859	0.738	0.102	0.010
	MB4	0.707	0.500	0.104	0.011
Average		0.849	0.728	0.100	0.010

<Table C.2> Marker Variable Analysis to Evaluate Common Method Bias

Factors	Uncorrected	$R_{MI} = 0.024$	
		M1	<i>t</i>
r (NWRC, PS)	-0.146	-0.174	-2.327
r (NWRC, DC)	-0.144	-0.172	-2.298
r (NWRC, SN)	-0.175	-0.204	-2.739
r (NWRC, DN)	-0.379	-0.413	-5.963
r (NWRC, MB)	-0.414	-0.449	-6.605
r (PS, DC)	0.423	0.409	5.892
r (PS, SN)	0.417	0.403	5.786
r (PS, DN)	0.195	0.175	2.341
r (PS, MB)	0.351	0.335	4.677
r (DC, SN)	0.592	0.582	9.413
r (DC, DN)	0.424	0.410	5.910
r (DC, MB)	0.500	0.488	7.348
r (SN, DN)	0.385	0.370	5.236
r (SN, MB)	0.482	0.469	6.990
r (DN, MB)	0.596	0.586	9.514

Note: NWRC, non-work-related computing intention; PS, punishment severity; DC, detection certainty; SN, subjective norms; DN, descriptive norms; MB, moral beliefs; M1, organizational commitment; R_{MI} , correlation between M1 (marker variable) and NWRC.

<Table C.3> Correlation Tables of Marker Variable and Study Constructs

Constructs	NWRC	PS	DC	SN	DN	MB	M1
NWRC	1.000						
PS	-0.146	1.000					
DC	-0.144	0.423	1.000				
SN	-0.175	0.417	0.592	1.000			
DN	-0.379	0.195	0.424	0.385	1.000		
MB	-0.414	0.351	0.500	0.482	0.596	1.000	
M1	0.024	0.253	0.194	0.207	0.158	0.241	1.000

Note: NWRC, non-work-related computing intention; PS, punishment severity; DC, detection certainty; SN, subjective norms; DN, descriptive norms; MB, moral beliefs; M1, organizational commitment.

◆ About the Authors ◆



Tserendulam Munkh-Erdene

Tserendulam Munkh-Erdene received her Master degree in MIS from Daegu Univeristy in Korea. She had work experiences in Golomt Bank in Mongolia. Her research interest lies in the human factors in IS security.



Sang Cheol Park

Sang Cheol Park is currently an assistant professor of the Department of Business Administration at Daegu University in Korea. He received his Ph.D. in MIS from Sungkyunkwan University in Korea. His research focuses on the areas of judgement and decision making in technology usage context, interorganizational systems in supply chain context, and (de) escalation in IT project management and so on. His papers have been published in the *Journal of AIS*, *Information Systems Journal*, *European Journal of Information Systems*, *Journal of Global Information Management*, *Computers in Human Behavior*, *Journal of Computer Information Systems* and among others.

Submitted: May 23, 2019; 1st Revision: August 2, 2019; Accepted: August 17, 2019