Revista Argentina de Clínica Psicológica
2020, Vol. XXIX, N°1, 39-49
DOI: 10.24205/03276716.2020.6

EFFECTS OF SANCTION ON THE MENTALITY OF INFORMATION SECURITY POLICY COMPLIANCE

Lin Chen[1], Jie Zhen[2],*
Kunxiang Dong[3], Zongxiao Xie[4]

Abstract

The employees' violation of information security policy (ISP) poses a major threat to the information resources of the employer. This paper constructs an integrated framework based on the theories on rational choice and general deterrence, and applies it to explain effects on sanction on ISP violation by employees. The model was tested by a scenario-based experiment on 320 employees from two universities and three companies in China. The results show that the certainty, severity and celerity of sanction have positive impacts on ISP compliance; the relationship between sanction severity and ISP compliance is mediated by the cost of noncompliance, and sanction celerity. The research findings have important theoretical and practical implications on the ISP compliance.

Key words: *Information Security Behaviors, Information Security, Behavior Intention.*
Received: 10-01-19 | Accepted: 23-05-19

INTRODUCTION

Employees' compliance with information security policies (ISP) is generally considered a key point in information security management (D'Arcy, Havav, & Galletta, 2009; Johnston, Warkentin, & Siponen, 2015; Siponen & Vance, 2010). Information security policy compliance refers to employees' behavior or intention to compliance with information security policies, procedures, or guidelines. Recent surveys report that employees' violation of ISP is among the top five causes of most information security incidents (Kolkowska, Karlsson, & Hedström, 2017). For instance, 131653 pieces of user data in www.12306.cn (he only official website of China Railway Customer Service Center) were leaked by hackers through Collision Attacks due to software bugs that were not fixed promptly in December 2014.

Several studies on information system security (ISS) or behavioral information security have investigated ISP compliance and violation (Crossler, Johnston, Lowry et al., 2013). In addition, researchers exploring information security issues have based on a variety of models, including protection motivation theory (Boss, Galletta, Lowry et al., 2015; Johnston & Warkentin 2010), neutralization theory (Siponen & Vance, 2010; Siponen, Mahmood, & Pahnila, 2014), and social control (Hsu, Shih, Hung et al., 2015). Deterrence theory is a widely used model (D'Arcy & Herath, 2011), especially when explaining workplace delinquencies. Although extant models help articulate the relation between sanctions and ISP compliance and violation, two noticeable gaps remain in prior research.

First, research that address ISP compliance uses different avenues (D'Arcy & Herath, 2011). Studies on criminology show that perceived certainty of punishment or sanction and delinquencies have a stable relationship (Vold, Bernald, & Snipes, 2002). Inconsistent findings are more evident in the context of information security than in ISP compliance. For instance, Johnston, Warkentin, & Siponen, (2015)

[1]College of Humanity and Law, Shandong University of Science and Technology, Qingdao 266590, China. [2]School of Business Planning, Chongqing Technology and Business University, Chongqing 400067, China. [3]School of Management Science & Engineering, Shandong University of Finance and Economics, Jinan 250014, China. [4]China Financial Certification Authority, Beijing 100054, China.
E-Mail: chenlynnqd@163.com

indicated that the effect of informal sanctions on ISP compliance is not significant, but Siponen & Vance (2010) showed that informal sanctions positively influence ISP compliance. This discrepancy may be ascribed to a misfit of method and question, moderation or interaction effects (D'Arcy & Herath, 2011), or the different constructs (Guo, 2013). The current study focuses on exploring the interactive influences of sanction celerity, certainty, and severity.

Second, Elliott, Feman, O"Day et al. (1985) argued that a single theory can explain only 10%–20% of violations, and different theories are responsible for the distinct part. He suggested that researchers should integrate theories to improve the predictive capability of the model. Meanwhile, deterrence theory does not concern the motivation to violate ISP. Thus, Paternoster & Simpson (1996) introduced rational choice theory (RCT) to complement deterrence theory. RCT mainly explores how potential offenders measure the costs and benefits in a particular environment (Vold, Bernald, & Snipes, 2002). However, the conventional framework of integration is inadequate for understanding violations in the context of information security.

Building on prior research, our focus on mediating and moderating roles makes at least two basic contributions to the literature. On the one hand, the study helps understand the mechanism of sanction influences on ISP compliance and how offenders measure the associated costs and benefits. On the other hand, we explore sanction celerity as moderator to adjust the relationship between sanction severity and certainty and ISP compliance.

THEORY FOUNDATION AND HYPOTHESES

Precious Work on Deterrence Theory

Deterrence theory can be traced to On Crimes and Punishments and come in two basic types: general deterrence theory (GDT) and special deterrence theory (SDT). GDT is designed to reduce people's engagement in undesirable activities, whereas SDT aims to only deter the individual offender from continuing to commit further crimes.

GDT suggests that the likelihood of individuals to commit a crime is reduced if the potential risks outweigh the benefits. This theory posits an individual will not be highly likely to commit a crime if they believe that the risk of getting caught is high (sanction certainty), severe penalties will be applied (sanction severity), and punishment will be swift (sanction celerity) (Johnston, Warkentin, & Siponen, 2015). These three central tenets, namely, sanction certainty, severity, and celerity, are closely related to ISP compliance. Sanction certainty refers to the likelihood of sanctions for violation behaviors of ISP, sanction severity is the harness of sanctions after security breach, and sanction celerity is the swiftness by which a specific sanction is implemented.

Criminal motivation, that is, the reason people choose to engage in undesirable activities, is not involved in deterrence theory. The original model focuses on analyzing a situation after a crime, thereby lacking predictive capability. Thus, in the 1970s, criminology studies began to investigate the causes of crime using different theories. For example, reasons that certain people commit crimes were investigated using the theory of learning, whereas self-control theory was used to explain why most individuals do not commit crimes.

After the rise of positivism, according to Gibbs (1968), the interest of criminology research returned to deterrence theory. Sources of data for research were primarily archival, such as the FBI annual crime statistics. However, using archival data has the disadvantage of regression because it can only verify correlation but not causation. Thus, research on deterrence theory gradually adopted an experimental research method.

The effect of sanction certainty on crime occurrence rate shows a stable relationship in criminology research. However, the relationship between sanction and crime occurrence rate is uncertain (Vold, Bernald, & Snipes, 2002; Nagin, 1998). Certain findings even show that death penalty is not a deterrent; however, figures suggest otherwise (Vold, Bernald, & Snipes, 2002). An increasing amount of evidence indicates that excessively violent crimes are associated with antisocial personality disorder, from which we assume that deterrence theory applies only to the rational man. This assumption offers the possibility of integrating deterrence and rational choice theories.

Research Advances of Deterrence Theory in Information Security Context

Straub (1990) introduced deterrence theory into information system (IS) research. According to Siponen, Willison, & Baskerville, (2008), only 48 out of 1,280 papers they analyzed adopted one or more theories, and 6 of these used GDT. This theory is the most widely applied model in the ISS context (Crossler, Johnston, Lowry et al., 2013; D'Arcy & Herath, 2011). However, no consistent conclusion is available for the roles of sanction certainty and severity in influencing ISP compliance. Table 1 summarizes the GDT-related journal articles.

Guo (2013) claimed that using different constructs

as the dependent variables, such as computer abuse, IS abuse (D'Arcy, Havav, & Galletta, 2009), and technological misuse, was one of reasons that certain research findings were inconsistent with previous ones. To address this issue, we select ISP compliance as the dependent variable, which is consistent with prior research, including those by Herath & Rao (2009), Chen, Ramamurthy, & Wen (2012), Siponen & Vance (2010), and Guo & Yuan (2012). Additionally, diverging independent variables have emerged. Certain papers used the construct of the extended deterrence model. For instance, Siponen & Vance (2010) and Johnston, Warkentin, & Siponen (2015) used formal/informal sanction. To solve this problem, Bernard & Snipes (1996) advised that researchers should focus not only on theory but also the relationship among different variables. In accordance with classic deterrence theory, we use three dimensions (certainty, severity, and celerity) to describe sanction in the current study.

Sanction Certainty and Severity and ISP Compliance

In Table 1, only Herath & Rao (2009a) and Chen, Ramamurthy, & Wen (2012) confirmed that sanction certainty has a significant positive impact on ISP compliance. Analysis of the questionnaires used in existing research shows that the measurement of variables may have a few biases. Most of the respondents are not IT professionals; therefore, they cannot fully understand the scenario of them. Generally speaking, the narrower the concept, the easier it is for respondents to understand. For example, Herath & Rao (2009) replaced sanction certainty with detection certainty, whereas Chen, Ramamurthy, & Wen, (2012) substituted it with certainty of control. We assert that certainty obliges opportunists to abandon violation intentions. Several extant studies also support this statement.

Whereas sanction certainty is ensured by technological solutions, sanction severity is generally a management issue. For example, organizations can deploy monitoring systems to observe appropriate behaviors (Herath & Rao, 2009). In this case, sanction certainty relies on IT equipment and policies ensure sanction severity. Many researchers found that sanction severity can restrain violations, which is in line with the general logical deduction (D'Arcy, Havav, & Galletta, 2009; Cheng, Li, Li et al., 2013). Meanwhile, white-collar employees are assumed to be rational people. Hence, we propose the following hypotheses.

Table 1. **GDT-related journal articles**

Studies	Main conclusions	Methods
D'Arcy, Havav, & Galletta, (2009)	Severity→IS misuse, (-) Certainty→IS misuse, NS	Scenario-based experiment
Herath & Rao (2009a)	Severity→ISP compliance, (-) Detection certainty→ISP compliance, (+)	Survey
Siponen & Vance (2010)	Formal sanction→Violation, NS Informal sanction→Violation, NS	Scenario-based experiment
Hu, Xu, Dinev et al. (2011)	Severity→Violation, NS Certainty→Violation, NS Celerity→Violation, NS	Survey
Son (2011)	Severity→Compliance, NS Certainty→Compliance, NS	Survey
Chen, Ramamurthy, & Wen, (2012)	Punishment→Compliance, (+) Reward→Compliance, (+) Control certainty→Compliance, (+)	Scenario-based experiment
D' Arcy & Devaraj (2012)	Severity→Technology misuse, (-) Certainty→Technology misuse, (-)	Survey
Guo & Yuan (2012)	Organizational sanction→Violation, NS Workgroup sanction→Violation, (-) Self-sanction→Violation, (-)	Scenario-based experiment
Cheng, Li, Li et al. (2013)	Severity→Violation, (-) Certainty→Violation, NS	Scenario-based experiment
Johnston, Warkentin, & Siponen (2015)	Formal sanction certainty→Compliance, NS Formal sanction severity→Compliance, NS Informal sanction certainty→Compliance, (+) Informal sanction severity→Compliance, (+)	Survey

Notes: NS indicates not statistically significant; (+) indicates positive; and (-) indicates negative.

H1: The level of sanction certainty (S. Certainty) is positively associated with information security policy compliance (ISP Compliance).

H2: The level of sanction severity (S. Severity) is positively associated with information security policy compliance (ISP Compliance).

Moderating Role of Sanction Celerity

Sanction celerity is seldom investigated in criminology and IS research (D'Arcy & Herath, 2011). Gibbs (1968) argued that the only rationale for an emphasis on celerity is in experimental psychology, particularly in operant behavior and classical (Pavlovian) conditioning. Most early criminologists held this view until Nagin & Pogarsky (2001) proposed the use of the time value of money as an economical basis for celerity. However, in the practice of information security, a main purpose of sanctioning is fostering employee habits. Sanction celerity is important for correcting the bad habits of employees. For instance, unattended electronic equipment should have their screens locked. If errant behavior is not promptly corrected, then employees might develop the wrong habits. This scenario fits Pavlovian conditioning. Hence, the following hypothesis is proposed.

H3: The level of sanction celerity (S. Celerity) is positively associated with information security policy compliance (ISP Compliance).

Many researchers have explored the cause of inconsistent findings about the influence of sanction severity and certainty on ISP compliance from different perspectives. D'Arcy & Herath (2011) suggested that the inconsistent findings of prior studies show a moderating or interaction effect among sanction certainty, severity, and celerity. For instance, Mendes (2004) found that the effect of sanction severity is better than that of sanction certainty for risk-averse potential offenders and the opposite for risk-takers. Meanwhile, utilitarians do not believe that they will be caught (Grasmick & Bryjak, 1980); thus, sanction severity and certainty have little or no effect on them. Chen, Ramamurthy, & Wen (2012) examined the interaction among punishment, reward, and certainty of control in the context of information security.

Early criminologists did not adopt celerity as a separate dimension of sanction. However, they believed that delay may weaken or diminish the efficacy of a deterrent (Nagin & Pogarsky, 2001). If a sanction is delayed, other staff may draw conclusions that they overestimate the magnitude of the sanction. In this regard, sanction celerity can reduce employees' perceived sanction severity and certainty. From the SDT perspective, executing the sanction quickly can decrease the probability of repeating the mistake. In other words, decreased sanction celerity may cause sanction severity and certainty to lose expected efficacy. Hence, we propose the following hypotheses:

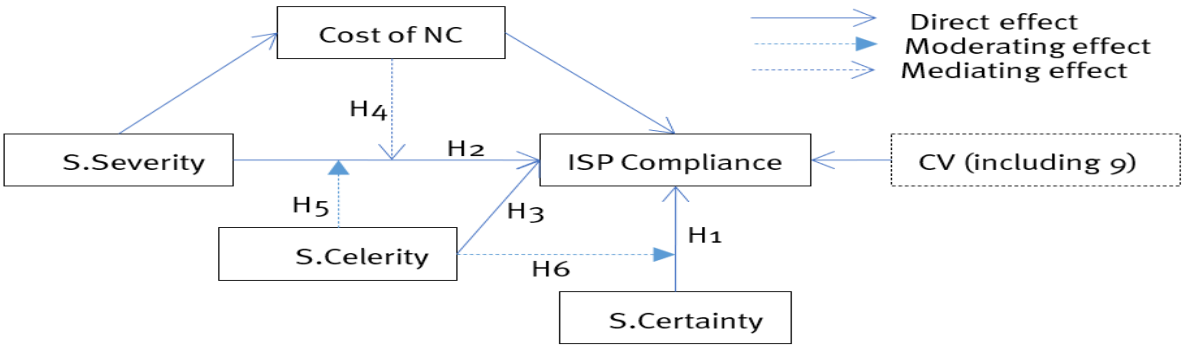
H5: The impact of sanction severity (S. Severity) on information security policy compliance (ISP Compliance) is moderated by sanction celerity (S. Celerity).

H6: The impact of sanction certainty (S. Certainty) on information security policy compliance (ISP Compliance) is moderated by sanction celerity (S. Celerity).

Mediating Role of RCT (Cost of Noncompliance)

Becker (1968) suggested that potential offenders rationally calculate the costs and benefits of committing a crime. The implicit premise of RCT is that offenders are not different from ordinary people. This premise does not deny the existence of unconscious violations or irrational crime, such as antisocial behavior, but explains the motive of offenders in specific circumstances (Vold, Bernald, & Snipes, 2002). In short, RCT is used to explain the motive for the crime.

Figure 1. **Diagrammatic sketch of research method**



Bulgurcu Cavusoglu, & Benbasat (2010) showed that ISP compliance is significantly influenced by benefit of compliance, cost of compliance, and cost of noncompliance. Hu, Xu, Dinev et al. (2011) indicated that perceived extrinsic/intrinsic benefits significantly impacts ISP violation. They used different dimensions of RCT. The present study focuses on the mediating role of RCT; hence, we select only cost of noncompliance to simplify the model. A Chinese saying talks about using heavy penalty in rough times, which means that harsh sanction is necessary, especially when the sanction certainty is low. Severe sanction can increase the cost of crime for offenders. Hence, setting aside sanction certainty, sanction severity impacts the cost of noncompliance, which ultimately affects ISP compliance. Thus, we propose the following hypothesis:

H4: The impact of sanction severity (S. Severity) on information security policy compliance (ISP Compliance) is mediated by the cost of noncompliance (Cost of NC).

Considering the above argument, an integrated model based on GDT and RCT is constructed, as shown in Figure 1.

DATA AND METHODOLOGY

Experiment Design

A scenario-based experiment was the most appropriate method for this study for the following reasons. (a) Data on information security violations are hard to obtain due to confidentiality. Almost all organizations keep information security incident data classified (Thaw, 2011) unless disclosure is mandated. (b) The occurrence of response bias may be increased if we directly asked the respondents about negative issues. Participants prefer to provide socially desirable answers rather than reveal their "unethical" intentions or behaviors. Hypothetical scenarios can partly avoid potential evaluation apprehension bias (Chen, Ramamurthy, & Wen, 2012; Siponen & Vance, 2010). A scenario-based experiment is a feasible means of learning the attitudes of respondents about sensitive topics (Nagin & Pogarsky, 2001; Paternoster & Simpson, 1996; D'Arcy, Havav, & Galletta, 2009; Chen, Ramamurthy, & Wen, 2012).

We conducted a 2x2x2 mixed design. Participants were randomly allocated to a scenario. To manipulate the independent variable effectively, only one violation behavior was committed in each scenario, such as personal use of instant messaging during working hours. Every scenario describes the ISP of a hypothetical company called "DaDu Co., Ltd." and the salary of a hypothetical employee named "Andy".

The first part of the survey was designed for capturing the participants' perception of sanction severity, certainty, and celerity and their intentions of complying. The second part was dedicated to the control variables, and the last part included basic information about the respondents. Furthermore, to avoid having inconsistent constructs (Guo, 2013), which may reduce the significance of the research, all independent and dependent variables were measured using 5-point Likert scale items mainly adopted from D'Arcy, Havav, & Galletta, (2009), Herath & Rao (2009), and Chen, Ramamurthy, & Wen, (2011). The items are provided in Table 3 and Appendix C.

Control Variables

Individual characteristics affect ISP compliance; control variables include gender, age, and education (Chen, Ramamurthy, & Wen, 2012). The respondents' organizational characteristics needed to be controlled. Paternoster & Simpson (1996) found that deterrence measures are more effective for managers than for general staff. D'Arcy & Herath (2011) argued that position is a relevant contingency variable. Following D'Arcy, Havav, & Galletta, (2009), organizational size (Org. Size) and organizational type (Org. Type) were included as control variables. Classified protection of IS (CPIS) is a mandatory standard in China that aims to improve the security awareness of employees in state-owned enterprises. Therefore, we controlled organizational ownership (Org. Ownership). The participants' individual and organizational characteristics are all provided in Table 3. The respondents' understanding of ISP might affect their intention to comply. If their organization has impeccable ISP, then the respondent has sufficient security awareness. Therefore, we controlled organizational ISP (Org. ISP) and individual operational security (Indi. OpSec), as provided in Table 4.

Data Collection

A total of 320 respondents completed the experiment, as shown in Table 2.

Table 2. **Characteristics of participants**

		Organization	Location
129	MBA students	University	Tianjin, China
45	MBA students	University	Beijing, China
75	Employees	Commercial bank	Beijing, China
51	Employees	IT company	Beijing, China
20	Employees	Public sector	Beijing, China

Approximately 64.7% of the respondents were

male probably because 29.7% of the participants came from IT-related organizations, in which more males than females are engaged. A summary of the demography of the participants is in Table 3.

Table 3. **Demographic characteristics of participants**

		Survey (n=320)	
Gender	Male	207	64.7%
	Female	113	35.3%
Age	18–24	8	2.5%
	25–34	227	70.9%
	35–44	69	21.6%
	45–54	12	3.8%
	55 and over	4	1.3%
Education	High school or lower	9	2.8%
	College	212	66.3%
	Master	83	25.9%
	PHD	16	5.0%
Position	Managerial	99	30.9%
	Administrative staff	44	13.8%
	IT managers	36	11.3%
	Professional staff	83	25.9%
	Others	58	18.1%
Org. Size	1–99	78	24.4%
	100–199	89	27.8%
	200–299	43	13.4%
	300–799	109	34.1%
	More than 799	1	0.3%
Org. Type	Consulting	17	5.3%
	Financial	79	24.7%
	IT	95	29.7%
	Manufacturing	7	2.2%
	Energy	26	8.1%
	Real estate	14	4.4%
	Research or education	14	4.4%
	Others	68	21.2%
Org. Ownership	State-owned	140	43.8%
	Private	97	30.3%
	Joint or foreign-funded	83	25.9%

Table 4. **Test results for cross-loading, validity, and reliability (N=320)**

Item	*ISP Compliance*	*Cost of NC*	*Org.ISP*	*Indi.OpSec*	M	SD
ISP Compliance_1	**0.866**	-0.424	0.245	-0.350	3.32	1.418
ISP Compliance_2	**0.856**	-0.440	0.309	-0.393	3.49	1.237
ISP Compliance_3	**0.824**	-0.451	0.307	-0.365	3.39	1.339
Cost of NC_1	-0.498	**0.861**	-0.190	0.286	3.46	1.216
Cost of NC_2	-0.565	**0.855**	-0.165	0.238	3.51	1.211
Cost of NC_3	-0.553	**0.855**	-0.091	0.310	3.57	1.280
Cost of NC_4	-0.506	**0.836**	-0.160	0.314	3.34	1.211
Org. ISP_1	-0.424	-0.390	**0.849**	0.315	3.38	1.329
Org. ISP_2	-0.408	-0.304	**0.785**	0.315	3.25	1.256
Org. ISP_3	-0.354	0.011	**0.665**	0.387	3.45	1.283
Org. ISP_4	-0.268	-0.033	**0.626**	0.344	3.57	1.372
Indi. OpSec_1	0.307	0.279	0.483	**0.813**	3.02	1.543
Indi. OpSec_2	0.303	0.174	0.401	**0.793**	3.21	1.473
Indi. OpSec_3	0.363	0.113	0.456	**0.781**	2.59	1.334
Indi. OpSec_4	0.108	-0.001	0.442	**0.621**	2.90	1.333
Indi. OpSec_5	0.092	0.036	0.429	**0.604**	2.91	1.365
Indi. OpSec_6	0.071	0.196	0.391	**0.600**	2.92	1.347
% of Variance	36.870	19.447	7.254	6.761	/	/
Cumulative%	36.870	56.317	63.570	70.332	/	/
Cronbach's alpha	0.925	0.918	0.832	0.837	/	/

ANALYSES AND RESULTS

We performed an exploratory factor analysis to assess the validity and reliability of four latent variables. As shown in Table 4, all factor loadings exceed 0.6 (McKnight, Choudhury, & Kacmar, 2002), cumulative proportions are greater than 70%, and the *Cronbach's alpha* values of the constructs all exceed 0.8 (Nunnally, 1978).

To check the manipulation of the independent variables, one-way ANOVA was performed. Sanction severity, celerity, and certainty were considered the independent variables, and the corresponding manipulation check questions were the dependent variables. The results are provided in Table 5. The manipulation of the three independent variables was correctly interpreted by the respondents as anticipated.

Table 5. **Manipulation checks of independent variables**

Construct	Low	High	F-Value (*df*)
	Mean (SD)	Mean (SD)	
S. Severity	2.71(1.21)	3.30(1.22)	17.80***(1,312)
S. Certainty	2.96(1.12)	3.60(1.06)	28.12***(1,312)
S. Celerity	2.74(1.03)	3.32(1.21)	20.03***(1,312)

Notes: 1) SD = standard deviation; *df* = degrees of freedom. 2) ***p<0.001.

We first applied ANOVA to test the direct and moderating effects. As hypothesized, the direct effects of sanction certainty, severity, and celerity are all significant. Sanction celerity has a moderating role in the relation between sanction certainty and ISP compliance but does not play the same role between sanction severity and ISP compliance. The results are shown in Table 6.

Furthermore, to explain how sanction celerity moderates the relation between sanction severity and certainty and ISP compliance, we explored the impact difference between the high and low levels of sanction severity and certainty and ISP compliance under high and low sanction celerity conditions. As shown in Fig. 2 (left), when sanction celerity is low, sanction certainty has no significant impact on ISP compliance ($t(152)=0.43$, $p=0.668>0.05$; $M_{low\ S.\ Celerity,\ low\ S.\ Certainty}=3.28$, $M_{low\ S.\ Celerity,\ high\ S.\ Certainty}=3.20$); when sanction celerity is high, sanction certainty has a significant impact on ISP compliance ($t(151)=3.71$, $p<0.001$; $M_{high\ S.\ Celerity,\ low\ S.\ Certainty}=3.28$, $M_{high\ S.\ Celerity,\ high\ S.\ Certainty}=3.20$). H6 was therefore supported. However, H5 was not supported. As seen in Fig. 2 (right), the impact of the difference between the high and low levels of sanction severity on ISP compliance is statistically the same under high and low levels of sanction celerity.

Table 6. **Test results (ANOVA for direct and moderating effects)**

NO.	Hypotheses	SD	F-Value	P-Value
H1	S. Certainty → ISP Compliance	5.19	4.05	0.045*
H2	S. Severity → ISP Compliance	8.41	6.56	0.011*
H3	S. Celerity → ISP Compliance	7.09	5.53	0.019*
H5	S. Severity × S. Celerity → ISP Compliance	0.42	0.33	0.569
H6	S. Certainty × S. Celerity → ISP Compliance	5.85	4.56	0.033*

Note: *p<0.05; **p<0.01; ***p<0.001.

We used regression to test the hypotheses. As shown in Table 7, H1-3 were supported, and the results of $H_{5\text{-}6}$ are consistent with those in Table 6. According to Baron & Kenny (1986), we examined the mediating role of the cost of noncompliance between sanction severity and ISP compliance. The result showed that cost of noncompliance played a full mediation role and H4 was supported (M1-3). All test results are provided in Table 7.

By synthesizing Tables 6 and 7, H1-3 were all supported; sanction certainty, severity, and celerity influence ISP compliance significantly. The findings confirmed the efficacy of GDT in the context of information security, although findings in criminology research are inconsistent, especially in death penalty research. We inferred that GDT was not suitable for offenders with extreme personality conditions, such as antisocial personality disorder. Employees are generally considered rational. However, we must point out that our findings are inconsistent with those of certain extant studies. We summarize the results in Table 8 and give our interpretation.

We argue that the differences may be caused by three factors. First, the discrepancies may be attributable to the different methods used. Second, sanction may lead to "reactance," which occurs when a person feels threatened by rules or regulations that may eliminate behavioral freedom. Third, some studies used constructs that differ from ours, such as computer abuse or IS misuse.

Figure 2. **Diagrammatic sketch of research method**

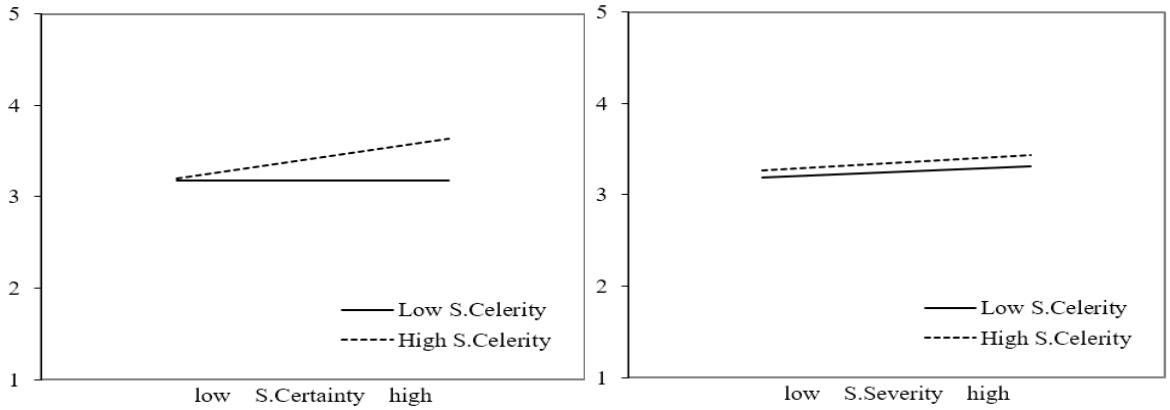


Table 7. **Test results (including all hypotheses and additional analyses)**

	DVs	M_1		M_2		M_3	
		ISP compliance		Cost of NC		ISP compliance	
		Beta	T	Beta	t	Beta	t
H1	S. Certainty	0.11	2.01*	0.10	1.87	0.05	1.19
H2	S. Severity	0.13	2.56*	0.12	2.27*	0.07	1.58
H3	S. Celerity	0.12	2.35*	0.14	2.67**	0.05	1.08
H4	Cost of NC					0.52	11.04***
H5	S. Severity × S. Celerity	0.03	0.57	-0.03	-0.60	0.05	1.05
H6	S. Certainty × S. Celerity	0.11	2.14*	0.14	2.67**	0.04	0.82
	(Additional Analyses)						
	S. Severity × S. Certainty	-0.16	-3.03**	-0.08	-1.37	-0.12	-2.71**
	S. Severity × S. Certainty × S. Celerity	0.04	0.78	0.06	1.08	0.01	0.24
	Org. ISP	0.22	3.19**	0.244	3.49**	0.09	1.53
	Indi. OpSec	0.14	2.02*	0.02	0.28	0.13	2.21*
	Gender	-0.04	-0.66	0.02	0.36	-0.05	-1.01
	Age	0.06	1.15	-0.03	-0.59	0.08	1.73
CVs	Education	0.01	0.13	0.03	0.46	-0.01	-0.14
	Position	-0.06	-1.13	-0.01	-0.09	-0.06	-1.27
	Org. Size	-0.02	-0.36	0.06	1.00	-0.05	-1.06
	Org. Ownership	-0.11	-2.03	-0.03	-0.51	-0.10	-2.08
	Org. Type	-0.10	1.91*	0.08	1.47	0.06	1.32

Note: * p<0.05; **p<0.01; *** p<0.001.

Table 8. **Comparison with prior studies**

Studies	Consistent?	Notes
Straub (1990)	Yes	Computer abuse is similar to ISP violations.
D'Arcy, Havav, & Galletta, (2009)	Severity, Y	The finding on severity is consistent with ours.
	Certainty, N	IS misuse is similar to ISP violations.
Herath & Rao (2009a)	Severity, N	The findings on severity are opposite ours. The discrepancy may be attributed to difference in methods.
	Certainty, Y	The finding on certainty is consistent with ours, although the constructs are slightly different.
Siponen & Vance (2010)	N	Their constructs vary from ours.
Hu, Xu, Dinev et al. (2011)	N	The discrepancy may be attributed to difference in methods.
Chen, Ramamurthy, & Wen (2012)	Y	Although they used different constructs, the findings are consistent with ours.
Johnston, Warkentin, & Siponen (2015)	Y	The finding on informal sanction is consistent with ours.

The cost of noncompliance mediates the relationship between sanction severity and ISP compliance (H4); that is, sanction severity affects the cost of noncompliance and ultimately affects ISP compliance. Table 6 also indicates that the cost of noncompliance also mediates the relation between sanction celerity and ISP compliance, but the same is not true for sanction certainty (*M_2: Beta = 0.10, p =1.87 > 0.05*). The moderating roles in Table 7 show that H5 and H6 were supported, consistent with Table 6. We also provided additional analyses. The impact of the difference between high and low levels of sanction severity under low-sanction-certainty conditions was smaller than that under high sanction certainty.

DISCUSSION

Contributions and Implications

This study contributes to the literature by adopting the cost of noncompliance (dimensions of RCT) to understand how sanction (GDT) influences ISP compliance and investigating the moderating role of sanction celerity on sanction severity and certainty. First, according to D' Arcy & Herath (2011)'s suggestion that "future research can explore the interactive influences of the certainty, severity, and celerity dimensions," we tested the moderating role of sanction celerity, which can partly explain the inconsistent findings of prior studies. Our findings about moderating role also provided additional evidence and new perspectives for other research areas, such as criminology, in exploring inconsistent consequences. Second, the cost of noncompliance plays a full mediation role in the relation between sanction severity and ISP compliance. We explained how sanctions influence ISP compliance. Integrations of GDT and RCT were implied to be necessary because of the existence of this full mediation effect. In addition, this study confirmed that sanction celerity influences ISP compliance significantly and provided new evidence for the effect of sanction severity and certainty. This evidence resolved, to a certain extent, the argument of D' Arcy & Herath (2011) that "future research should incorporate celerity of sanctions into IS deterrence frameworks." For scarce investigation of sanction celerity, our results can be applied to research on wrongdoings such as prevention of cheating in examinations.

Our findings also have important implications for practice. First, sanction celerity is the most feasible way to improve ISP compliance. Sanction certainty usually depends on technical methods, which need added expenditure. Although improving sanction severity can be achieved through policies, it involves many regulation compliance issues, such as the Employment Contract Act. Moreover, sanction celerity plays a moderating role between sanction certainty and ISP compliance. By improving sanction celerity, the effects of sanction certainty impact on ISP compliance are also strengthened. Therefore, enterprises should develop mechanisms to ensure sanction celerity. Second, the cost of noncompliance plays a full mediating role between sanction severity and ISP compliance but not in the relation between sanction certainty and ISP compliance. This finding showed that organizations should improve sanction severity and certainty so that "every violation will be sanctioned." At the same time, organizations should not only improve sanction severity but also pay attention to improving employees' perceived cost of noncompliance.

Limitations and Future Research

Our study inevitably has its limitations. Like most empirical studies in IS research and criminology, the first limitation is the use of compliance/violations intention instead of actual behaviors. Although supported by the theory of planned behavior and numerous prior studies (D'Arcy, Havav, & Galletta, 2009), a discrepancy exists between actual behaviors and behavioral intentions. Therefore, using actual behavior in future studies may shed light on this important issue. The second limitation is the sample. A total of 146 of respondents came from banks or IT-related organizations, which are more concerned with information security than other industries. As seen in Table 6, organizational ISP (Org. ISP) and individual operational security (Indi. OpSec) are all positively associated with ISP compliance. Future research can include additional contingency variables.

CONCLUSIONS

Despite the abundant studies on GDT in the context of IS research, a research gap remains, namely, how employees decide on compliance and violation using trade-off analysis. By adopting RCT to explain motivations, we constructed an integrated framework that is based on GDT and RCT and applied scenario-based experiments to investigate our hypotheses. First, sanction celerity plays a moderating role between sanction severity and certainty and ISP compliance. This finding can partly account for the cause of inconsistent results of extant research. Second, the cost of noncompliance mediates the relation between sanction severity and ISP compliance, which explains how sanctions influence ISP compliance. Third, the

results showed that sanction certainty, severity, and celerity are all positively associated with ISP compliance.

Acknowledgement

This research is supported by the National Social Science Foundation of China(17CGL019).

REFERENCES

Baron, R. M., & 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.

Becker, G. S. (1968). Crime and punishment: And economic approach. *The Journal of Political Economy*, 76(2), 169-217.

Bernard, T. J., & Sinpes, J. B. (1996). Theoretical integration in criminology. *Crime and Justice*, 20, 301-348.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.

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.

Chen, Y., Ramamurthy, K., & Wen, K. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157-188.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. G. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, 39(6), 447-459.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warhentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32(2), 90-101.

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

D'Arcy, J., Havav, 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.

Elliott, J. H., Feman, S. S., O"Day, D. M., & Garber, M. (1985). Hereditary Sclerocornea. *Archives of Ophthalmology*, 103(5), 676-679.

Gibbs, J. P. (1968). Crime, punishment, and deterrence. *Southwestern Social Science Quarterly*, 48(4), 515-530.

Grasmick, G. H., & Bryjak, G. J. (1980). The deterrent effect of perceived severity of punishment. *Social Forces*, 59(2), 471-491.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, 32(1), 242-251.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, 2012, 49(6): 320-326.

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

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

Hsu, S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. *Information Systems Research*, 26(2), 282-300.

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

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through. *MIS Quarterly*, 39(1), 113-134.

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems*, 26(1), 39-57.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334-359.

Mendes, S. M. (2004). Certainty, severity, and their relative deterrent effects: Questioning the implications of the role of risk in criminal

deterrence policy. *Policy Studies Journal*, 32(1), 59-74.

Nagin, D. S. (1998). Criminal deterrence research at the outset of the twenty-first century. *Crime and Justice*, 23(1), 1-42.

Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, 39(4), 865-892.

Nunnally, J. C. (1978). Psychometric Theory. New York: McGraw-Hill. 1978.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, 30(3), 549-583.

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., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217-224.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *International Conference on Information Systems*, 26-38.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, 48(7), 296-302.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276.

Thaw, D. B. (2011). Characterizing, classifying, and understanding information security laws and regulations: Considerations for policymakers and organizations protecting sensitive information assets. UC Berkeley Electronic Theses and Dissertations, University of California, Berkeley. 2011.

Vold, G. B., Bernald, T. J., & Snipes, J. B. (2002). Theoretical criminology (5th Edition). Oxford University Press. 2002.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computer & security, 38, 97-102.