Journal of Management Information Systems

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/mmis20

Organizations' Information Security Policy Compliance: Stick or Carrot Approach?

Yan Chen [a], K. Ramamurthy [b] & Kuang-Wei Wen [c]

[a] College of Business Administration, University of Wisconsin-La Crosse

[b] Sheldon B. Lubar School of Business, University of Wisconsin-Milwaukee

[c] Information Systems Department, University of Wisconsin-La Crosse

Published online: 09 Dec 2014.

To cite this article: Yan Chen , K. Ramamurthy & Kuang-Wei Wen (2012) Organizations' Information Security Policy Compliance: Stick or Carrot Approach?, Journal of Management Information Systems, 29:3, 157-188

To link to this article: http://dx.doi.org/10.2753/MIS0742-1222290305

Organizations' Information Security Policy Compliance: Stick or Carrot Approach?

YAN CHEN, K. (RAM) RAMAMURTHY, AND KUANG-WEI WEN

Yan Chen is a visiting assistant professor at the College of Business Administration, University of Wisconsin–La Crosse. She received her Ph.D. in management science, specializing in management information systems, from the University of Wisconsin–Milwaukee. Her work has focused on information security, security tool interface and issues, and e-commerce. Her research has been published in the *International Journal of Electronic Business* and a number of refereed conference proceedings. Her paper was nominated for the best student paper award at the Sixth International Conference on Design Science Research in Information Systems and Technology (DESRIST 2011). She is a member of the Association for Information Systems and the Decision Sciences Institute.

K. (Ram) Ramamurthy is a professor and Roger L. Fitzsimonds Distinguished Scholar in management information systems at the Sheldon B. Lubar School of Business, University of Wisconsin–Milwaukee. He received his Ph.D. in business with a concentration in MIS from the University of Pittsburgh. He has 20 years of industry experience, having held several senior technical and executive positions. He served as an associate editor of *MIS Quarterly* for four years. His current research interests include electronic commerce and business; adoption, assimilation, and diffusion of modern IT; data resource management and data warehousing; systems security compliance; IT business value; IT outsourcing; decision and knowledge systems for individuals and groups; systems security; and total quality management, including software quality. He has published 50 research articles in major scholarly journals, including *MIS Quarterly, Journal of Management Information Systems, IEEE Transactions on Software Engineering, IEEE Transactions on Systems, Man and Cybernetics, Decision Sciences, European Journal of Information Systems, Decision Support Systems, Information & Management, Journal of Organizational Computing and Electronic Commerce, International Journal of Electronic Commerce,* and *IEEE Transactions on Engineering Management,* and over 29 articles in refereed conference proceedings. He is a charter member of the Association for Information Systems.

Kuang-Wei Wen is a professor and chair of Information Systems Department at the University of Wisconsin–La Crosse, the department he established in 1999. He received his Ph.D. in architecture, decision and information systems from the Carnegie Mellon University, and an M.S. from the University of Wisconsin–Milwaukee. His main research focuses on global study of e-value creation among small and medium-sized enterprises, information security management, application of artificial intelligence to Web site customization, and effective use of social computing. His research has been published in scholarly journals, including *Management Science, European Journal of Operational Society,* and *International Journal of Electronic Business,* plus more than 30 refereed articles in conference proceedings.

Journal of Management Information Systems / Winter 2012–13, Vol. 29, No. 3, pp. 157–188.

ISSN 0742–1222 (print) / ISSN 1557–928X (online)
DOI: 10.2753/MIS0742-1222290305

Abstract: Companies' information security efforts are often threatened by employee negligence and insider breach. To deal with these insider issues, this study draws on the compliance theory and the general deterrence theory to propose a research model in which the relations among coercive control, which has been advocated by scholars and widely practiced by companies; remunerative control, which is generally missing in both research and practice; and certainty of control are studied. A Web-based field experiment involving real-world employees in their natural settings was used to empirically test the model. While lending further support to the general deterrence theory, our findings highlight that reward enforcement, a remunerative control mechanism in the information systems security context, could be an alternative for organizations where sanctions do not successfully prevent violation. The significant interactions between punishment and reward found in the study further indicate a need for a more comprehensive enforcement system that should include a reward enforcement scheme through which the organizational moral standards and values are established or reemphasized. The findings of this study can potentially be used to guide the design of more effective security enforcement systems that encompass remunerative control mechanisms.

Key words and phrases: coercive control, compliance theory, general deterrence theory, information security policy, punishment, remunerative control, reward.

It has long been a well-recognized fact that companies' information security efforts are threatened by employee negligence and insider breach (e.g., [44]). Information security cannot be assured by using technological solutions alone. To deal with the "insider" issues, companies have started to focus on various management and control mechanisms such as security policies, procedures, and enforcement in addition to continually updating their security technologies [13, 18, 34, 61]. In the meantime, under increasing pressure from various stakeholder action groups interested in security and privacy concerns, the U.S. government and a few security conscientious industries have stepped in by introducing specific regulations and standards. As a result of their intervention, having a security policy in place is quite common among companies that are required to comply with regulations and mandates such as the Payment Card Industry Data Security Standard (PCI DSS), Gramm–Leach–Bliley Act, Sarbanes–Oxley Act, and Health Insurance Portability and Accountability Act (HIPAA) [30]. Regardless of this trend, however, human beings are still the weakest link in the information security chain. A recent survey of over 500 security professionals in U.S. corporations, government agencies, medical institutions, and universities that was conducted by the Computer Security Institute [56] reported that the average monetary loss per respondent was $288,618, and that 44 percent of the respondents reported insider security-related abuse, making it the second-most frequently occurring computer security incident (virus and malicious software infection incidents being the most frequent). Similar results were found by the 2008 information security breaches survey sponsored by the Department for Business, Enterprise, and Regulatory Reform (BERR) in the United Kingdom [34]. The average cost experienced by a UK company's single securitycompromised incident was between £10,000 and £20,000. For very large businesses, this cost was between £1 million and £2 million. Furthermore, 62 percent of the worst security incidents had an internal cause [34]. Clearly, employees could just bypass their company's security policies in order to get their job done more conveniently even if they were aware of their company's published security policies [72].

Employees do not seem motivated to follow security policies and procedures. They appear to more often follow their well-honed habits and day-to-day routines and are resistant to behavioral changes [10, 33]. They often use "neutralization" techniques or make excuses for their policy violations [61]. Since effective information security requires employees to comply with established security policies and procedures, the area of information security management that focuses on issues such as effectiveness and cost of security policy enforcement, balance between productivity and strict security, and between security level and information technology (IT) budget has become one of the top areas of security concerns for businesses [56].

To address the compliance concern, different strategies for effective security policy enforcement have been proposed. Drawing on the general deterrence theory (GDT) [65, 66], scholars usually advocate the negative enforcement strategy—*punishment.* The GDT proposes that as punishment certainty and severity increase, unwanted behaviors can be deterred [33, 65, 66]. But, borrowing from theories in organizational literature, some scholars support the positive enforcement strategy—*reward.* Some argue that reward provides needed incentive and motivation for compliance [10] and that reward combined with sanction is one of the important factors that can influence individual employees' rational cost–benefit assessment of compliance vis-à-vis noncompliance behaviors [13].

From a control perspective, both reward and punishment are control mechanisms to achieve organizational goals [21]. To be effective, such control mechanisms need to tie into the certainty of how often those control mechanisms are enforced or materialized. *Certainty of control,* referring to the probability of the enforcement strategy materializing, has been an influential factor that may contribute to the effectiveness of the enforcement strategy of policy compliance (e.g., [5, 33, 65, 66]). However, to the best of our knowledge, no prior studies in information systems (IS) have examined the interaction effects between punishment and reward for enforcing security policy compliance. Moreover, the empirical findings regarding the influence of reward on security policy compliance in the IS security literature are inconsistent: rewards were not found to affect compliance intention or actual compliance in some studies (e.g., [10, 51]), whereas rewards were found to significantly influence an employee's belief in the benefit of security policy compliance (e.g., [13]). Thus, the difference in the effectiveness of these two enforcement strategies is far from clear in the IS field. In addition, although the choice between punishment and reward has long been an important and interesting topic in other fields such as social psychology and organizational management, even in these well-established fields, research findings are still not in agreement. In particular, the joint effects of punishments and rewards are even more unclear [4, 24]. Finally, the interaction effects between punishment/reward and certainty of control are also not clear in the IS security literature, although some recent attention has been given to the joint effects of punishment and certainty of control (e.g., [61]).

Motivated by those shortcomings in the literature, we believe it will be revealing to understand the different effects and interaction effects (if any) of the two enforcement strategies as well as the main and interaction effects (if any) between the two enforcement strategies and certainty of control in the context of security policy compliance. Drawing on the compliance theory [22] and GDT [65, 66], this study investigates these two enforcement strategies and their interaction in the context of security policy compliance. The main variables of interest are *severity of punishment, significance of reward,* and *certainty of control.* Our central research questions are

> *RQ1: How does punitive enforcement affect employees' security policy compliance?*
>
> *RQ2: How does rewarding enforcement affect employees' security policy compliance?*
>
> *RQ3: How does enforcement certainty affect employees' security policy compliance?*
>
> *RQ4: What is the combined effect of punitive and rewarding enforcement on employees' security policy compliance?*

The rest of the paper is organized as follows. In the next section, a literature review related to reward and punishment in organizations and in IS security is discussed, and the significance of this study is elaborated. The third section draws on the major elements of the general deterrence and compliance theories to develop the study's six hypotheses. In the fourth section, the research design for examining the study's hypotheses is presented. The data analysis and results are presented in the fifth section and discussed in the sixth section. The final section discusses the contributions and implications of this study for research and practice in IS security as well as its limitations and future research extensions.

Literature Review

Using negative stimuli (punishment or sanction) to discourage undesirable behaviors or using positive stimuli (reward) to encourage desirable behaviors has long been a topic in fields such as education, social psychology, and organization. Nevertheless, studies in these fields have so far not reached a consistent conclusion about the effectiveness of punishment or reward on the investigated behavior. Some scholars argue that incentives/rewards do not work and that punishment is a better choice for deterring commitment of a deviant act, whereas others believe in "the redemptive power of reward" [40, p. 54]. On the punishment side, Arvey and Ivancevich [5] pointed out that there were two different points of view about punishment in the organizational behavior and management literature. Some studies have shown that punishment is not a high priority choice for managerial application because the presumed negative consequences may outweigh any benefits it renders [59]. It is reasoned that the use of punishment by an organization would result in undesirable emotional side effects such as anxiety, aggressive acts, or withdrawal. Moreover, employees might display hostility toward and retaliate against the punishing agent in the organization. However, empirical evidence found in other studies indicates that these presumed side effects are particularly weak and might occur only in situations where the punishing agent administers punishment indiscriminately. Arvey and Ivancevich [5] further pointed out that punishment is a frequent and naturally occurring event in all of our lives and that it shapes a large part of our psyche and behavior. Therefore, a careful examination of punishment, particularly factors influencing the effectiveness of punishment, is necessary. Sims [59] argued that reward tends to have a much stronger effect on employee performance and that punishment tends to be more of a result than a cause of employee behavior. Proponents of punishment argue that punishment may serve to uphold social norm within an organization, signal appropriate and inappropriate behaviors to employees, and deter deviant acts [70]. Therefore, punishment as a deterrent strategy can actually result in positive outcomes.

Researchers and practitioners in the IS literature also recommend the use of deterrent strategy against undesirable behavior such as computer abuse and noncompliance of security policy. Drawing on theories in criminology, the GDT has been used in studies on preventing and reducing computer abuse in organizations (e.g., [16]). Computer abuse is a major source of security incidents that accounts for 50 percent to 75 percent of all incidents originating from within an organization, and it causes significant financial losses to the organization [16]. It has been found that direct punishment associated with computer abuse leads to a decrease in abuse intention on the part of employees when the perceived certainty of enforcement and perceived severity of punishment increase. Straub [65] surveyed 1,211 organizations and found that besides preventive security software, deterrent administrative procedures that focused on disincentives or sanctions against computer abuse resulted in significantly lower computer abuse. In two subsequent studies, Straub and his colleague [64, 66] provided similar suggestions that punishment or disciplinary procedures can deter computer abuse.

At the same time, to promote desirable behaviors and improved performance, employers often use rewards. But, as with punishment, the effect of reward has been challenged by scholarly research. According to the control theory, control is an important facet of organizational design. A critical aspect of exercising control is a formally documented statement articulating desirable behaviors or outcomes. Control can be accomplished through evaluation and reward. Reward signals to employees that their work or behaviors meet the expectations of the organization [10, 21]. Eisenhardt [21] argued that in organizations, reward is implicit. She noted that an organization's emphasis on rewards can capture "the reward linkage of control arrangements" [21, p. 138].

Reward can be viewed as a contract through which an organization can exercise its control through intangible rewards (e.g., potential promotion, honor of being the employee of the month) and tangible rewards (e.g., bonus and vacation). Eisenhardt further pointed out that "the contracting emphasis makes rewards explicit" [21, p. 138]. Not surprisingly, many scholars in organizational management believe that the proper use of rewards as a means of controlling and managing behaviors and performance can benefit organizations in various ways, such as directing employees' behaviors, motivating employees, promoting excellence, attracting and retaining talent, and increasing job satisfaction (e.g., [28, 77]). Furthermore, when compared to punishment, reward is capable of creating harmonious instead of hostile relations in organizations.

However, the positive effects of reward have also been challenged by critics (e.g., [2, 40]) for a number of reasons. First, rewards may just facilitate temporary compliance. It is a version of extrinsic motivators that seldom alter the attitudes that underline employees' behaviors and do not create a lasting commitment [40, 58]. Once rewards are gone, employees may revert to their old behaviors. Second, rewards have punitive side effects. Employees may experience feelings of being controlled or manipulated by managers. As a result, rewards could create a controlling, not a motivating, work environment [40]. Rewards could also generate tense or hostile relations in an organization. Because outcomes or performance are not easily programmable or measurable given the complexity of tasks in organizations, a phenomenon of "divergence of preferences (i.e., people side of control)" could occur [21, p. 136] when rewards are to be decided. Determining how to reward is a judgment call by managers that depends on their perspectives, values, and experiences. As a result, individual employees could often be rewarded for the wrong things or not rewarded for the right things because of divergence of preferences [6]. One of the worst situations could be a manager rewarding employees not based on performance but on his or her personal relationship with those employees. In addition, employees often perceive rewards as being drawn from a fixed or scarce resource pool; more for one person often means less for another [77]. Therefore, reward could produce damaging reactions. Finally, rewards can push employees to aim at individual gains instead of organizational goals [9]. Suppose the performance of the chief executive officer (CEO) of a company is evaluated in terms of the stock price of the company and that his or her benefits, reputation, and annual bonus depend on the performance. The CEO may manipulate the stock price in order to have "look-good" performance, whereas his or her action actually may be hurting the company. So, performance-based corruption control is emerging as an organizational challenge [27].

Researchers and practitioners in the IS security literature also recommend reward as a control mechanism for compliance. Boss et al. [10] pointed out that persistent issues regarding compliance to security policies and procedures indicate that not all employees of an organization regard those policies and procedures as mandatory and, therefore, do not comply with them. In addition, the fact that security policies and procedures are put in place does not necessarily mean that employees will interpret and comply with those policies and procedures collectively and continue to adhere to them over time. Rewards can send strong and additional signals to employees that compliance with security policies and procedures is mandatory [10]. Recent research [13] also suggests that reward, along with other types of benefits and costs, is an influencing factor when employees make a rational choice of compliance or noncompliance. Thus, rewards can help to enforce security policy compliance.

Because of undesirable side effects of punishments alone or rewards alone, many organizations use both coercive and remunerative mechanisms in conjunction with other control mechanisms to enforce compliance [22]. Many scholars (e.g., [4]) also believe that rewards and punishments are distinct forces to promote desirable behaviors in social exchanges and that rewards and punishments interact. However, findings regarding the joint effects of rewards and punishments remain inconsistent in previous research. Andreoni et al. [4] found that punishments and rewards jointly have a significant influence on cooperation, but punishments alone or rewards alone have little or no influence on it. Nevertheless, Fehr and Schmidt [24] surprisingly did not find the significant interaction of bonuses and fines on the agents' effort to carry out the principles' contracts.

Given the importance of security policy compliance for securing organizations from various types of attacks and that reward and punishment are two common policy enforcement strategies, it is necessary to understand if the effectiveness of these strategies is different within the context of security policy compliance and, if so, in what ways. In addition, inconsistent findings about the effectiveness of reward and punishment from studies in other fields also suggest that we need further research on the issue to provide more empirical evidence for organizational management to make the right decision on security policy enforcement strategy.

Theoretical Frames and Hypotheses Development

The compliance theory of Etzioni [22] points out that compliance, which is a central element in organizations, refers to members of organizations acting as per their organizational directives. To enforce compliance, organizations in general exercise three types of control: coercive, remunerative, and normative [22]. In coercive control, organizations use threats and punishments ("the stick") as a means to regulate compliance and punish noncompliance. Remunerative control refers to a policy instrument by which organizations use some forms of economic incentives ("the carrot"), such as bonus, promotion, and commissions, in exchange for members' compliance. When it comes to normative control, symbolic and moral reasoning behind compliance and values of compliance are emphasized [8, 22, 48]. Etizioni's [22] definition of coercive control is limited to the application or threat of physical force and pain, and he defined remunerative control as the power of controlling material resources. More recently, from a resource dependence perspective [54], researchers argue that coercive control means using negative reinforcement strategy—depriving resources valuable to employees upon noncompliance, while remunerative control rests on positive reinforcement strategy—stratifying employees with the addition of resources in exchange for compliance [67]. Following this more practical perspective, we view that coercive control is control of punishment and remunerative control is control of rewards [15]. Organizations generally do not depend on just one type of control to enforce compliance. Indeed, most organizations employ all three types of control, while each organization may apply a different amount of each type of control. The choice of organizational control to enforce compliance is complicated since, along with many

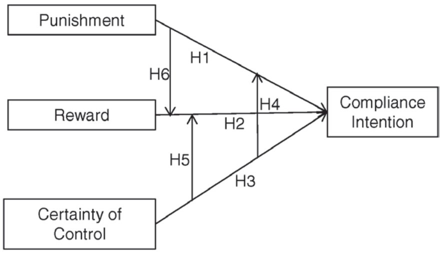


Figure 1. Research Model

other organizational factors, the three types of control mechanisms themselves may interact with each other to affect compliance.

In the field of information security policy compliance, coercive control with its underpinning in the GDT from criminology dominates research and practice (e.g., [16, 35, 64, 65, 66]), while the effect of normative control, such as moral reasoning, on employees' information security policy compliance has also been found (e.g., [48]). Remunerative control, in general, is missing in the field of information security policy compliance, although it has drawn some attention recently (e.g., [10, 13]). Moreover, we know little about the different effects of reward, punishment, and their interaction on compliance intention when both of these control mechanisms are in place.

Conceptually, both coercive control and remunerative control belong to formal forms of control, and normative control can be termed as an "informal form of control." In formal control, written documents in terms of rules, goals, procedures, and regulations are in place to specify desirable behaviors, while in normative control, organizational values, norms, and cultures are emphasized to influence compliance [17]. Since formal control is dominant in organizations, we take it as the focus of this study.

With the above reasoning, we synthesize the compliance theory with the GDT by introducing remunerative control—that is, reward—in this study. We propose that both punishment and reward, certainty in enforcing these options, and the interactions of these factors influence employees' intention to comply with information security policy. The research model is shown in Figure 1.

Punishment

As noted, the GDT suggests that sanctions or punishments could serve as a deterrence mechanism against deviant behavior. This theory assumes that when potential violators are aware of organizational efforts to control undesirable behaviors, they are less likely to commit a deviant act. The efforts of sanction or punishment are measured by two subconstructs: severity of punishment and certainty of punishment [65]. Severity of punishment refers to the degree of punishment associated with not complying with security policy, and certainty of punishment refers to the probability of being punished. If potential violators realize that the likelihood of being punished is high and penalties are severe for violation, they are more likely to be deterred from engaging in undesirable acts and to adhere to desirable acts. Otherwise, they may engage in such deviant acts because benefits from pursuing such acts may be great. For instance, surfing on the Internet in the workplace is more enjoyable than doing work, and sharing the password among project team members is convenient. Findings in punishment research also suggest that for punishment to be effective in organizations, it must start out at a relatively severe level (e.g., [5]). They point out that in organizational contexts, moderate or severe punishment may be more effective in coping with undesirable behaviors than mild or no punishment. Hence,

> *Hypothesis 1: The level of punishment for not complying with security policies is positively associated with the intention to comply with security policies.*

Reward

There is both theoretical and empirical evidence that rewards can motivate employees to improve performance, productivity, creativity, and compliance (e.g., [20, 22, 43]). According to the agency theory, the agents (employees) are rational and self-interested and, therefore, may act to maximize their own outcomes without extending effort toward achieving the principal's (the organization's) goals [9, 43]. Reward structures, when properly designed, can facilitate harmonizing the goals of agents and their principal. Thus, rewards can be useful for altering the agents' behaviors to realize the principal's goals.

Control theory also suggests tying rewards to desired behaviors [10, 21, 38]. Even if security policies are stated and employees' compliance is evaluated, compliance could be poor in the absence of proper rewards for compliance. Employees could interpret that security policies are not important and mandatory because compliance or noncompliance makes no difference [10]. It may be noted that compliance with security policies and procedures is traditionally not a part of merit-pay schemes that assess performance [10] and rewarding security policy compliance may not yet be common in organizations [13]. However, the importance of reward in promoting compliance intentions and behaviors (e.g., [13]) and in signaling moral standard of compliance [10] has increasingly been discussed in the IS field. In addition, prior research on ethical conduct and compliance management has found that even if performance of ethical conduct and compliance is hard to measure, employees' perceptions that ethical conduct and compliance are valued and would be rewarded are critical to create an ethical culture that can significantly improve the effectiveness of compliance programs [71]. Similarly, to promote compliance in organizations, using rewards to demonstrate that desirable behaviors are recognized may create a security compliance culture and thus significantly improve compliance [26]. Therefore, we would argue that without rewards, the control signal for compliance to security policies and procedures could be weak, and thus, desirable behaviors are not reinforced. A reward system tied to security compliance sends a strong signal that compliance is mandatory, and thus increases the intention to comply with stated security policies.

Hypothesis 2: The level of reward for complying with security policies is positively associated with the intention to comply with security policies.

Certainty of Control

In both the punishment and reward literature, prior research suggests that certainty of punishment or reward could directly affect the effectiveness of punishment or reward. Employees analyze and infer the level of certainty based on how they interpret the timing, schedule, and contingence of punishment and reward. Arvey and Ivancevich [5] argue that the timing and schedule of punishment are two important determinants of the effectiveness of punishment. Punishment is more effective in deterring undesirable behaviors if the punishment is imposed immediately and it consistently occurs after each undesirable behavior is observed than if the punishment is delayed or it is inconsistently imposed. In other words, if employees realize that their noncompliance behaviors are continuously monitored and punished immediately and consistently, their intention to comply with security policies will increase.

The IS security literature also indicates that to effectively deter noncompliance behaviors, monitoring such behaviors and imposing penalties upon detection are necessary [33, 65]. Simply having security policies in place will do little to change employees' noncompliance behaviors if they believe those policies are not enforced [53]. An organization's deterrence efforts directly influence the employees' corresponding compliance behaviors. If employees are aware that their organization never really values their compliance behavior and never investigates their noncompliance behaviors, they may adhere to any current noncompliance behaviors because the chance of being caught is low. High certainty of control sends signals to employees of the organizational efforts to monitor, evaluate, and punish noncompliance behaviors. Consequently, their intentions to comply will increase because the chance of being caught and being punished is high.

Further, in a rewards policy context, organizational research has found that "instrumentality," referring to a belief of the likelihood that the employee will obtain the reward if he or she meets the performance expectation, is an influential factor on motivation [74]. Policies stating the certainty that performance will result in rewards augment the instrumentality [74]. Thus, we argue that linking certainty to reward is often essential to shaping and maintaining desirable behaviors and attitudes toward such behaviors.

From a control perspective, both reward and punishment are control mechanisms to achieve organizational goals [21]—specifically, in this study, compliance with security policies. Certainty of control is the probability of the enforcement strategy materializing. If employees believe there is high certainty of control associated with compliance or noncompliance, their intention to comply with security policies will increase. Hence,

Hypothesis 3: Certainty of control will positively influence the intention to comply with security policies.

Interactions: Punishment × Certainty of Control and Reward × Certainty of Control

Theories of decision making under uncertainty suggest that when people make a decision associated with an event, they look at not only the event itself but also the probability of the event. Their cognitive process tries to capture both the impact and the likelihood of the event. They make their decision based on a utility function [55]. Applied to the context of this study, when employees make a decision on whether to comply with their organization's security policies, they evaluate and implicitly factor the potential effects on their utility function of a loss (punishment) or gain (reward). However, they evaluate not only the potential positive (negative) effect of reward (punishment) but also the likelihood of reward (punishment). Moreover, organizations, as complex systems, exhibit nonlinear patterns such as interaction terms because in organizations almost each influential factor/event is related to a probability of occurrence [3]. To specify such patterns, it is critical to assign the probability of occurrence to the focal factor and examine their interaction terms [3].

Research in criminology points out that deterrence theory is based on a utilitarian perspective, and an "interaction hypothesis is more consistent with the utilitarian perspective" [31, p. 473] because sanction severity will have little or no effect on those who do not perceive they will be caught. Inconsistent findings about the impact of punishment severity and certainty from prior IS security research may further indicate the existence of an interaction effect between the two factors. Similarly, it is has long been observed that the effect of rewards is moderated by the probability of occurrence that rewards are offered [19]. To promote compliance, employees need to realize that no matter the sanctions or rewards, enforcement is real and compliance or noncompliance behaviors are acted upon [71]. Thus, we argue that the enforcement certainty influences an employee's judgment about the effectiveness of reward or punishment: the impact of the magnitude of difference in reward or punishment will be moderated by the certainty of control. Hence, we offer the following two hypotheses:

> *Hypothesis 4: The impact of punishment on the intention to comply with security policies is moderated by the certainty of control: the difference in impact on intention to comply between high and low levels of punishment contexts in high certainty of control environments is smaller than in low certainty environments.*

> *Hypothesis 5: The impact of reward on the intention to comply with security policies is moderated by the certainty of control: the difference in impact on intention to comply between high and low levels of reward contexts in high certainty of control environments is smaller than in low certainty environments.*

Notice that although it is tempting to simplify our model by multiplying reward and punishment by their respective certainties and thereby circumventing the factor interaction issue, we do not adopt this strategy for the reason of not making unsupported assumptions on employees' risk posture. Once reward (or punishment) is multiplied by the certainty factor to yield an expected value, continuing to use this value in the decision calculus would necessitate the assumption of risk neutrality in the preference of the employee. As such, the employee would be indifferent between a large reward with low certainty and a small reward with high certainty because both prospects bring the same level of expected value. This is, however, a rather unusual situation arising in real life among ordinary people. We believe the imposition of risk neutrality might be acceptable in cases where group preferences are modeled or the nature of risk aversion is not the central focus of decision making. For example, in Siponen and Vance's [61] study, the central focus was to build and validate the neutralization theory-based compliance model. Their use of expected penalty to simplify the deterrence theory components that exist only for nomological completeness of modeling appears to be of no real concern in their study. Yet the GDT is in the center of our model, and the interplay of reward/punishment with certainty must be explicitly explored in the absence of any assumption of risk posture of the employee.

Interaction: Punishment × Reward

Organizations as complex systems seldom use coercive control alone or remunerative control alone, but often use both to increase compliance [22]. It has long been observed that organizations as well as individuals often use a combination of rewards and punishments to enforce desirable relationships in social exchanges [4]. When both reward and punishment are in the policy enforcement scheme, the joint effect is not as simple as adding up the two effects or canceling each other. In many cases, punishment and reward interact with each other [22]. Prior research has found that punishments alone or rewards alone have little or no influence on cooperation, but jointly they have significant effects on cooperation [4]. Previous studies also found that punishment could cause retaliation and hostile emotional reactions and that these reactions can lead to strong resistance to compliance [46]. Sometimes, punishment is interpreted by employees as "duress" so that their "perceptions of dispositional causation" are diminished [32, p. 419]. Thus, adding a reward scheme to the punishment enforcement can reduce such strong emotional reactions since reward can encourage cooperation and boost self-esteem [4]. Furthermore, although many organizations predominantly use coercive control, those coercive control mechanisms do not result in desirable compliance behaviors unless they are used in conjunction with remunerative control mechanisms [22, 62]. Ethical and compliance programs might be more effective if they incorporate a reward system while having coercive control mechanisms in place to follow up and punish noncompliance [71]. In other words, the effect of punishment depends on reward. Further, if a person is threatened by punishment for noncompliance, then his or her decision to comply is constrained by the threat of punishment. To a certain extent, he or she has to comply because of the threat of punishment. But, if a person is offered reward for compliance, then his or her decision is less constrained. He or she has an option for giving up the reward in exchange for noncompliance [32]. Thus, when the reward level is low, the levels of punishment more dominantly influence compliance intention than when the reward level is high. Hence, we offer the following hypothesis:

> *Hypothesis 6: The impact of punishment on the intention to comply with security policies is moderated by reward: the difference in impact on intention to comply between mild and severe levels of punishment contexts in low levels of reward environments is greater than in high levels of reward environments.*

Research Methodology

Experiment Design

GIVEN THE NATURE OF THE HYPOTHESES UNDERLYING THIS STUDY, a Web-based experiment involving real-world employees in their natural settings was deemed the most appropriate. We used a 2 × 2 × 2 mixed design. The first factor, *punishment,* was administrated at two levels (severe and mild). The second factor, *reward,* was also administrated at two levels (high and low). The third factor, *certainty of control,* was varied at two levels (high and low). The first two factors, punishment and reward, are "within-subjects" factors, and the third factor, certainty of control, is a "between-subject" factor. A set of eight (four each for high and low certainty of control) scenarios was designed to test the main effects and interaction effects of these three factors. The participants were randomly assigned to two groups: one exposed to the four high level of certainty of control scenarios and the other to the four low certainty of control scenarios (between-subjects factor). Each set of the four scenarios reflected the combinations of the levels of the first two within-subject experimental factors, punishment and reward, as shown in Table 1. For example, Scenario 1 describes the manipulation of a low level of reward and the mild level of punishment. Scenario 2 describes the manipulation of the low level of reward and the severe level of punishment, and so forth. To control for any order effects due to repeated trials, we used the concept of a Latin square design to create a Latin square design matrix, as shown in Table 1. Each participant in the corresponding group was randomly assigned one of four presentation orders in the Latin square design matrix.

As to the experiment procedure, details of the security policies related to password, e-mail use, and Internet use of a hypothetical company (iCorp) were first presented to all of the participants. The participants were asked to assume that they were employees of this company and to thoroughly read and understand the policies. This was then followed by a series of four different case scenarios (for one of the two levels of certainty of control noted earlier to which they were assigned); the participants were asked to go through each scenario and then answer questions about their intention to comply with the security policies imposed in this hypothetical company, as well as to answer the manipulation check questions (see the Appendix, statements *MANI-C1, MANI-C2, MANI-P,* and *MANI-R*) after each case scenario. Finally, the participants were asked to answer a set of questions related to the control variables and demographic profiles.

Table 1. Latin Square Design Matrix

Order_1	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Order_2	Scenario 2	Scenario 3	Scenario 4	Scenario 1
Order_3	Scenario 3	Scenario 4	Scenario 1	Scenario 2
Order_4	Scenario 4	Scenario 1	Scenario 2	Scenario 3

Note: Scenario 1, low reward and mild punishment; Scenario 2, low reward and severe punishment; Scenario 3, high reward and mild punishment; Scenario 4, high reward and severe punishment.

As noted, a hypothetical scenario technique was employed in this experiment design. This research method has been widely used in IS research on a diverse range of topics such as software piracy [47], ethical IT use behavior [42], project escalation [37], conveying bad news to project managers [63], IT outsourcing risks [69], and risk perceptions in business process outsourcing [29]. Scenario-based techniques have been commonly used in studying ethics-related security behaviors such as security policy violation and computer abuse (e.g., [16, 61]). We made use of the scenario analysis technique for a number of reasons. One primary reason is the reluctance of and the resulting moratorium by real-world companies in allowing their employees to divulge information security–related information for competitive and credibility reasons. Another major reason is to avoid potential evaluation apprehension bias that prompts respondents to provide ethically or socially desirable answers rather than reveal their “unethical” intentions and behaviors (if any). Hypothetical scenarios that tell another person’s story may help respondents to drop their guard and reveal their true intentions [61]. We chose a design of multiple scenarios per respondent because each scenario is associated with a relatively small number of survey items [36]. Following the suggestions of scenario development in the literature [25, 75, 76], we used a fractional design in which each participant is given four scenarios to avoid possible information overload and fatigue. At the same time, we ensured that each participant was exposed to an adequate number of scenarios so that we could properly manipulate our independent variables [75]. We controlled the possible order and carryover effects by using a Latin square design matrix for the random assignment of scenarios [75]. We examined fairly extensively information security policy practices prevailing in industry [35] and surveyed the existing literature to ensure that our scenarios were realistic, familiar, and succinct, and that our corresponding findings were generalizable based on the scenarios. In addition, the scenarios were pilot tested and commented on twice by eight information security professionals and experts (see the Data Collection section for details on the pretests). Since no “optimal” number of scenarios has been suggested in the literature [76], we pilot tested the number of scenarios used in the study to ensure its adequacy.

Finally, to ensure validity and reliability [11] as well as compatibility with extant literature, the dependent variable, intention to comply with information security policy, was measured by three seven-point Likert scale items adopted from Herath and Rao [33], Ryan [57], and Venkatesh et al. [73] (see the Appendix).

Control Variables

It was necessary to control for influences of a number of variables to identify the true effects of the study variables considered here. Previous research in the IS security literature, for instance, suggests that individual characteristics such as age and gender are related to security policy compliance intention [41, 66]. Therefore, we included gender, age, and education as our control variables. Organizational security culture was also included as a control variable because of potential differences in security policy compliance among employees in different organizations [7, 16, 60]. For instance, in financial and health-care institutions, because of the overall critical nature of information security to the business, organizational security cultures may exist within which the value of information security is continually reinforced through daily practices and routine training. However, this might not be the case for some firms in the manufacturing sector that may place less value on information security. Even within the same industry (e.g., financial industry), financial institutions can vary in organizational security cultures. Therefore, we felt it necessary to consider and control for the organizational security culture, measured by eight seven-point Likert scale items adapted from Knapp et al. [39] (see the Appendix). In addition, we used organizational security culture to control for a possible normative control effect, although it is not the focus of this study. For the same reason, we controlled for the influences of organizational security practices—measured by organizational security policy, security training, and security monitoring, with four, four, and six seven-point Likert scale items, respectively, adopted from D'Arcy et al. [16] (see the Appendix).

Data Collection

Following good research principles and practices, we conducted two pilot tests in two U.S. Midwestern companies in the financial industry with eight information security professionals who are responsible for their company's information security policy implementation. Thus, we validated each of the three bilevel experimental factors as well as the eight case scenarios and questionnaire design. Necessary modifications and refinements based on the results of the two pilot tests were incorporated to ensure robustness of the research design. Then, we conducted a third pilot test on three IT professionals enrolled in an MBA class in a major university in the midwest, and further modifications and refinements were made based on the results of the test.

We recruited our participants from the same two midwest companies where the first two pilot tests were done. A total of 50 employees, 25 from each company, participated in our Web-based experiment; none of the pilot test participants were in this set. Each participant was given four trials that followed the previously mentioned design. Thus, the overall sample size for this research is 200, and each of the eight case scenarios has 25 observations.

Analyses and Results

Demographic and descriptive statistics of the participants show that there was a good distribution of age and educational background of the participants; the median age was about 35 years, and over 50 percent had at least an undergraduate degree. The participants had, on average, been with their firms for 7 years and in the profession for over 15 years. This profile suggests that the participants in this study were mature, educated, experienced, and knowledgeable; thus, their responses can be considered to be dependable and used with confidence. Because the number of female participants ($N_{\text{female}} = 33$) was more than twice the number of male participants ($N_{\text{male}} = 14$) (three employees did not reveal their gender), we tested for any significant difference in compliance intention between genders and found no significant difference ($p = 0.485$).

The convergent and discriminant validity of the four control constructs and the dependent construct were assessed by carrying out exploratory factor analyses (EFA) with varimax rotation of the extracted factors; this was followed by testing reliability of the constructs via examining the Cronbach alpha values. As per guidelines laid down in previous research [14, 45], we dropped indicator items with low loadings (less than 0.60) and with high cross loadings (greater than 0.40). The final loadings and cross loadings matrix from the EFA as well as the eigenvalues and Cronbach alpha values of the constructs are shown in Table 2.

The results of the emergent 5-factor structure met the above criteria, with all the predefined items loading on their corresponding latent variables (2 out of 27 indicators measuring the 5 constructs were dropped during scale refinement), supporting discriminant validity [45]. Among the 5 constructs, the minimal eigenvalue was 1.57 (for *compliance intention*), greater than the recommended value of 1, which verifies the convergent validity of each construct. All the Cronbach alpha values exceeded the cutoff value of 0.70 [50], thus supporting the reliability of all 5 constructs.

Manipulation checks of the independent variables—reward, punishment, and certainty—and of the order effect were performed by running one-way ANOVAs (analyses of variance). We first ran three one-way ANOVAs on the manipulation check questions of punishment (*MANI-P*), reward (*MANI-R*), and certainty (mean of *MANI-C1* and *MANI-C2*) by the two levels of reward, punishment, and certainty, respectively (see the Appendix for the details of manipulation statements *MANI-P, MANI-R, MANI-C1,* and *MANI-C2*). As shown in Table 3, the results provide strong evidence that the manipulations of the three independent variables were correctly interpreted by the participants as originally anticipated. The differences between the manipulations were all significant ($p < 0.001$). We then ran a one-way ANOVA on the dependent variable of compliance intention and manipulation check questions of reward, punishment, and certainty by the order shown in Table 1. The results presented in Table 4 show that the order of presenting the four scenarios had no significant effects on the major variables of this study ($p > 0.05$), except for *perceived severity of punishment.* The post hoc analysis shows that only Order 2 and 3 were marginally different from each other ($p = 0.069$). Therefore, we argue that our manipulations are successful and that the order effect is not an issue in this study.

Table 2. Validity (Joint Factor Analysis) and Reliability Test Results

Indicator items	F1: Security culture	F2: Security monitoring	F3: Security policy	F4: Security training	F5: Compliance intention
Complicance_Intent1	0.030	–0.009	–0.041	0.040	**0.934**
Complicance_Intent2	0.034	0.031	–0.005	0.059	**0.968**
Complicance_Intent3	0.009	0.146	0.029	–0.005	**0.932**
Security_Culture1	**0.756**	0.263	0.136	0.231	0.090
Security_Culture2	**0.769**	0.187	0.147	0.295	0.055
Security_Culture3	**0.817**	0.097	0.165	0.114	0.179
Security_Culture4	**0.902**	0.132	0.058	0.082	–0.031
Security_Culture5	**0.848**	0.128	0.023	0.321	–0.063
Security_Culture6	**0.669**	0.334	–0.032	0.503	0.175
Security_Culture7	**0.922**	0.119	0.157	0.009	–0.021
Security_Culture8	**0.811**	–0.067	0.071	–0.072	0.002
Security_Policy1	0.148	0.020	**0.936**	0.088	0.040
Security_Policy2	0.344	0.087	**0.779**	0.235	–0.009
Security_Policy3	–0.075	0.273	**0.695**	0.092	–0.033
Security_Policy5	0.055	0.045	**0.866**	0.192	0.031
Security_Training2	0.239	0.349	0.027	**0.744**	0.107
Security_Training3	0.117	0.207	0.287	**0.717**	0.036
Security_Training4	0.250	–0.110	0.191	**0.697**	–0.011
Security_Training5	0.160	0.261	0.377	**0.642**	–0.294
Security_Monitoring1	0.208	**0.616**	0.187	0.297	–0.080
Security_Monitoring2	0.150	**0.734**	0.103	0.111	–0.015
Security_Monitoring3	–0.030	**0.681**	0.295	0.326	0.153
Security_Monitoring4	0.142	**0.857**	–0.007	–0.094	0.140
Security_Monitoring5	0.099	**0.791**	0.101	0.299	0.117
Security_Monitoring6	0.278	**0.816**	–0.031	0.091	–0.143
Eigenvalue	10.239	3.549	3.129	2.823	1.571
Variance explained (percent)	35.31	12.24	10.67	9.94	5.42
Cumulative variance (percent)	35.31	47.55	58.33	68.07	73.49
Cronbach's alpha	0.950	0.882	0.863	0.823	0.956

Note: Items of a common factor appear together in boldface.

A repeated-measure ANOVA with a between-subjects factor was performed to test our hypotheses. The results in Table 5 show that the main effect of punishment was significant ($F_{1,48} = 5.07$, $p = 0.029$), supporting H1 that the severity level of punishment enforcement policy has a significant effect on policy compliance intention. The results strongly support H2 that the level of reward can significantly affect employees' compliance intention ($F_{1,48} = 12.73$, $p = 0.001$). H3, which tests the main effect of enforcement certainty, was supported as well ($F_{1,48} = 6.07$, $p = 0.017$). The two-way interaction between punishment and certainty of control was significant ($F_{1,48} = 3.12$, $p = 0.084$). Further, Plot A in Figure 2 indicates that the impact difference between the high and low levels of punishment condition in the high certainty of control condition was smaller than in the low certainty condition. Therefore, H4 was supported. The

Table 3. Manipulation Checks of Independent Variables

	Low certainty (n = 100)	High certainty (n = 100)		
Study variables	Mean (SD)	Mean (SD)	F-value (df)	Significant difference
Perceived severity of punishment	3.51 (1.76)	5.66 (1.68)	77.90*** (1, 198)	Yes
Perceived significance of reward	3.48 (1.83)	5.81 (1.28)	108.72*** (1, 198)	Yes
Perceived enforcement certainty	4.75 (1.46)	5.74 (1.23)	26.78*** (1, 198)	Yes

Notes: SD = standard deviation; df = degrees of freedom. *** $p < 0.01$.

two-way interaction between punishment and reward was also significant ($F_{1,48} = 7.67$, $p = 0.008$), strongly supporting H6.

Plot B in Figure 2 provides further graphical demonstration, supporting H6 that the impact of punishment on the intention to comply with security policies is greater when reward is low than when reward is high. However, the two-way interaction between reward and certainty of control (H5) was not supported ($F_{1,48} = 0.68$, $p = 0.414$), as shown in Table 5. Plot C in Figure 2 graphically shows that the impact difference between the high and low reward on compliance intention is statistically the same at the high and low levels of certainty of control. Note that since we pooled data from two organizations, we also ran a one-way ANOVA on the dependent variable of compliance intention and manipulation check questions of reward, punishment, and certainty level by organization type (the two organizations were coded as 2 and 3, respectively). The results show that participants from the two organizations were not significantly different on the major variables of this study ($p > 0.05$) except for *perceived certainty of control.* However, we still controlled for organization type in our analysis. All the control variables as well as organization type were initially input as covariates, and the results show that their main effects were insignificant; therefore, we did not include them in further analysis.

Discussion

Overall, the results confirm support for five of the six hypotheses, substantively supporting our theoretical model. As hypothesized, we found that the main effects of severity of punishment, significance of reward, and certainty of control were all significant. Beyond lending further support to the GDT that severity of punishment and certainty of punishment deter employees from security policy violation, the study's findings highlight that reward enforcement, a remunerative control mechanism in the

Table 4. Manipulation Check—Scenario Presentation Order by Study Variables

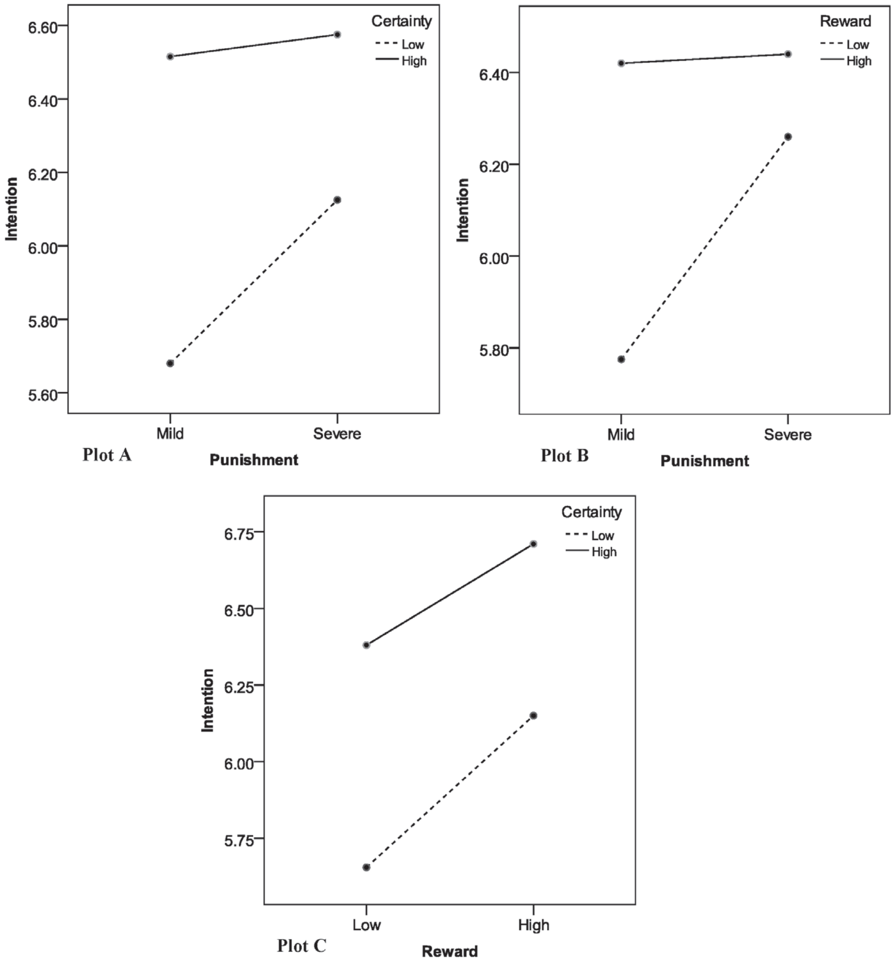
	Order-1 (*n* = 48)	Order-2 (*n* = 72)	Order-3 (*n* = 36)	Order-4 (*n* = 44)		
Study Variables	Mean (SD)	Mean (SD)	Mean (SD)	Mean (SD)	*F*-value (df)	Significant difference[1]
Compliance intention	6.19 (1.24)	6.19 (1.24)	6.37 (1.14)	6.19 (0.80)	$0.24^{n.s.}$ (3, 196)	None
Perceived severity of punishment	4.81 (1.79)	4.07 (2.14)	5.11 (1.97)	4.75 (2.00)	2.73* (3, 196)	2–3
Perceived significance of reward	4.38 (2.11)	4.75 (2.03)	4.64 (1.82)	4.77 (1.82)	$0.43^{n.s.}$ (3, 196)	None
Perceived enforcement certainty	5.02 (1.75)	5.42 (1.34)	5.04 (1.38)	5.37 (1.20)	$1.10^{n.s.}$ (3, 196)	None

Notes: SD = standard deviation; df = degrees of freedom. [1] Bonferroni as well as Scheffe tests of paired contrasts. * $p < 0.1$; n.s. = not significant.

Table 5. Summary of ANOVA Results and Hypotheses Test Results

Hypothesis	Mean square	*F*-value	*p*-value	Support?
H1: Punishment × Intention	2.35	5.07	0.029**	Yes
H2: Reward × Intention	7.61	12.73	0.001***	Yes
H3: Certainty × Intention	31.21	6.07	0.017**	Yes
H4: Punishment × Certainty × Intention	1.45	3.12	0.084*	Yes
H5: Reward × Certainty × Intention	0.41	0.68	$0.414^{\text{n.s.}}$	No
H6: Punishment × Reward × Intention	2.21	7.67	0.008***	Yes

Notes: df = 1, 48. * $p < 0.1$; ** $p < 0.05$; *** $p < 0.01$; n.s. = not significant.



Plot A

Plot B

Plot C

Figure 2. The Plots of Interaction Terms

IS security context, could be an alternative for organizations where sanctions do not successfully prevent violation. Indeed, our respondents' answers to an open, voluntary question at the end of the survey revealed that they dislike the "unmotivated atmosphere" caused by the "pure" sanction enforcement policy of their organization (see the comment below as one example). Such kinds of sentiments and dislike may be indicative of the ineffectiveness of coercive control in the current IS security policy compliance efforts:

> Our organization doesn't reward good practices on the computer, but will punish you. Very unmotivated atmosphere.

Another important finding is support for the interaction effect between severity of punishment and certainty of control. As two important factors of the GDT, their direct effects on IS security policy compliance intention and IS misuse intention have been studied before. However, little research in IS security has examined their interaction effect based on theories such as the prospect theory in risk management, according to which decisions regarding loss are jointly determined by the expected value of loss and the probability associated with it. This finding provides a new insight into the GDT and is consistent with a large body of research in other fields such as sociology and criminology. Specifically, when enforcement certainty is high, severity of punishment matters less because punishment now is not just a "gesture" any more.

Our results also highlight an important finding of the interaction effect between reward and punishment, confirming the asymmetrical effects of reward and punishment on compliance when both of these policies are in place. Plot B in Figure 2 shows that high reward as well as low reward makes little difference in compliance intention under the severe punishment condition as compared to the mild punishment condition. This finding indicates that when punishment is severe, adding a remunerative control mechanism may not affect compliance too much. When punishment is mild, a remunerative control mechanism may be a valuable add-on to increase compliance.

Interestingly, the effect of reward on compliance intention is not moderated by certainty of control. This finding is contrary to our prediction. A possible explanation could be that under current practices, remunerative control is, in general, not an enforcement mechanism for IS security compliance within organizations. In other words, employees would not be rewarded if they comply well with IS security policy. Therefore, we conjecture that the effect of reward on employees is more symbolic or psychological; a promise of reward for good compliance makes them feel good and empowered, and thus they would comply (at least in the short to medium term) no matter if the reward ends up being real or just a promise. A possible explanation is that employees' interpretation of the probability associated with a reward is not straightforward; they are likely to first build their belief in this probability and then connect it to the reward.

Finally, the finding that the main effects of all the control variables were insignificant is also interesting. In other words, the main and interaction effects of the three independent variables on compliance intention were the same across the two companies in this study despite some differences in terms of IS security culture and practice. In addition, age, gender, and education also made no difference. Based on our sample, this finding indicates generalizability of the main and interaction effects of the three independent variables for firms in the financial industry. However, given the unique characteristics of the two participating companies and possible unique industry characteristics, this finding requires further investigation. For example, we may find personal differences in terms of age, gender, and education to be relevant to compliance intention in other industries since personal differences could already have been neutralized by intensive IS security training programs commonly implemented in the financial industry.

Conclusions

Contributions and Implications

This study makes several theoretical contributions to academic research in IS security. First, this study introduces and incorporates both punishment and reward for enforcing IS security policy into the context of IS security research. To the best of our knowledge, no prior studies in IS security have compared how the two strategies with different levels of compliance certainty influence individual employee's compliance intention. Second, this study brings more attention to reward as a plausible strategy in the field of IS security. Drawing on the GDT, IS research has long been focused on punishment or sanction as the de facto enforcement strategy. Researchers believe that if policy violation is properly and promptly detected and then punished, future violations can be deterred (e.g., [16, 64, 65]). Building on the compliance theory, this study brings reward as an alternative strategy for enforcing IS security policy compliance to IS security researchers' attention, even though it may appear somewhat counterintuitive that rewards are offered for security compliance. Indeed, employees' outcome beliefs regarding reward play a significant role in influencing employees' compliance intention (e.g., [13]). This study provides further evidence that reward strategy for enforcing IS security policy compliance deserves further research. Finally, this study advances the GDT by empirically testing and confirming the interaction effect between punishment and certainty of control. The result shows that severity of punishment and certainty of enforcement of punishment jointly affect compliance intention in the GDT. Moreover, other interactions supported by this study also provide a new insight into theories regarding IS security policy compliance research.

The findings in this study have important implications for both research and practice. For practice, our findings can help organizations that are interested in improving information and systems security behaviors of their employees to design more effective enforcement systems that encompass portfolios of security enforcement strategies. For research, our findings offer significant support to prior studies that have suggested that employees' unethical behaviors are complex and caused by various reasons, and as such, a more comprehensive IS security policy enforcement system including more effective deterrence strategies than mere punishment or sanction will be needed. In particular, this study suggests that such a comprehensive enforcement system should include a reward enforcement scheme through which the organization's moral standards and values are established or reemphasized [12]. It may be necessary to explore additional theories about reward and further validate them in the context of IS security. Managers may use such reward schemes to raise employees' ethical awareness, which plays an important role in their moral decision making and actual behaviors [13, 48, 49]. When applying the results of our empirical study, managers would be wise to not only consider IS security a preventive function—punishing violation and then deterring noncompliance—but also put reward schemes in place to help increase individual employees' ethical awareness about IS security policy and, possibly, foster a common favorable disposition to compliance (ethical behaviors). In support of this viewpoint, we provide one example of a response to an open-ended voluntary question at the end of the survey that expressed the sentiment that good practice should be appraised and rewarded:

> I believe the company has high intention of safety practices, appropriate use of work computers, etc. but there are employees that completely disregard all company policies repeatedly without fear of being held responsible for their actions. The employees that adhere to guidelines have only their personal satisfaction of knowing they are following the "rules."

Moreover, given the interaction effect between reward and punishment found in this study, such reward schemes need to be carefully designed so that the new remunerative policy does not conflict with or cancel out the effect of existing coercive or other enforcement policies in place. Meanwhile, proper mechanisms for compliance assessment need to be put in place to prevent the harmful effect of "divergence of preferences" [21, p. 136], as noted in the Literature Review section. However, in the context of IS security compliance, a case of extreme excellence in compliance is much harder to make than a case of extreme excellence in performance in other contexts such as retailing. Besides, in some industries, due to stringent laws and regulations, 100 percent compliance is expected and even one instance of violation would not be tolerated. These difficulties might hinder the actual implementation of a monetary reward scheme. Therefore, organizations interested in introducing reward enforcement may need to consider intangible rewards such as written or oral commendation to enhance moral standards.

Limitations and Future Research

One limitation of this study is the sample, which included two companies in the financial industry, which is more stringently regulated in terms of information security than other industries such as, say, manufacturing. Care also needs to be taken when generalizing our findings to other companies in the financial industry. Our sample size of 50 participants (yielding 200 cases with a repeated measure) may be another limitation. However, our participants are from the real business world and participated in the experiment in their workplace, leaving no doubt about the representativeness of our sample for a population in the financial industry. A possible threat to the internal validity, which could exist in all within-subject designs, may be another limitation. However, following the suggestions in the literature, we took necessary precautions (see the Experiment Design section) to minimize the threat. In addition, since our data were collected in a cross-sectional manner, common method bias could be another limitation of this study. However, the data were used to test interaction effects in this study, thus mitigating this common data source problem [23]. Therefore, common method bias may impose a much smaller threat to this study. Moreover, we measured compliance intentions instead of actual behaviors. Although studying intention rather than actual behavior is common in the IS literature, it is still a potential limitation of the current study; people may not actually do what they state as their intentions, in this instance to comply with security policies [48]. Finally, although various precautions, such as ensuring anonymity of the survey participants and using a hypothetical company and scenarios, were taken to prevent potential evaluation apprehension bias, some respondents could still have provided socially desirable responses rather than their actual thoughts in the survey; note that the mean values of "intention to comply" were above five on a seven-point scale, reflecting perhaps a propensity to be seen as good corporate citizens (i.e., not violating security policies), although such high values have been observed in innumerable previous studies that have used the technology of acceptance, theory of reasoned action, and theory of planned behavior models (e.g., [1, 52, 68]). Moreover, respondents could have mixed up scenarios with their actual working environment and, therefore, did not reveal their actual intentions and behaviors. This is another possible limitation of the current study.

One direction future research could take is to conduct an action research type of study to further investigate how a new remunerative reward policy could affect compliance with information security policies in organizations. Action research would allow researchers to observe subtle organizational changes due to the introduction of the new remunerative policy and its effect on compliance. Another direction for future research is to duplicate this study in many more organizations from various/diverse industries beyond the financial sector considered here to ensure generalizability of our study's findings. While duplicating this research, we can further investigate how significantly the levels of reward interact with different kinds of organizations in terms of existing IS security culture and enforcement policy. Finally, future research could explore the interaction effects of coercive, remunerative, and normative controls in the context of information security in light of the argument that organizations in general exercise all these types of control, although the weights placed on each may vary across organizations [22], and given the findings that in the IS security context, establishing moral standards and preventing denial of personal responsibility play an important role in compliance attention [48, 61].

References

1. Agarwal, R.; and Karahanna, E. Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24,* 4 (2000), 665–694.

2. Amabile, T.M. How to kill creativity. *Harvard Business Review, 76,* 5 (1998), 76–87.

3. Anderson, P. Complexity theory and organization science. *Organization Science, 10,* 3 (1999), 216–232.

4. Andreoni, J.; Harbaugh, W.; and Vesterlund, L. The carrot or the stick: Rewards, punishments, and cooperation. *American Economic Review, 93,* 3 (2003), 893–902.

5. Arvey, R.D., and Ivancevich, J.M. Punishment in organizations: A review, propositions, and research suggestions. *Academy of Management Review, 5,* 1 (1980), 123–132.

6. Baker, G.P.; Jensen, M.C.; and Murphy, K.J. Compensation and incentives: Practice vs. theory. *Journal of Finance, 43,* 3 (1988), 593–616.

7. Banerjee, D.; Cronan, T.P.; and Jones, T.W. Modeling IT ethics: A study of situational ethics. *MIS Quarterly, 22,* 1 (1998), 31–60.

8. Bemelmans-Videc, M.-L.; Rist, R.C.; and Vedung, E. *Carrots, Sticks and Sermons: Policy Instruments and Their Evaluation.* New Brunswick, NJ: Transaction, 1998.

9. Bloom, M., and Milkovich, G.T. Relationships among risk, incentive pay, and organizational performance. *Academy of Management Journal, 41,* 3 (1998), 283–297.

10. Boss, S.R.; Kirsch, L.J.; Angermeier, I.; Shingler, R.A.; and Boss, R.W. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18,* 2 (2009), 151–164.

11. Boudreau, M.-C.; Gefen, D.; and Straub, D.W. Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly, 25,* 1 (2001), 1–16.

12. Brass, D.J.; Butterfield, K.D.; and Skaggs, B.C. Relationships and unethical behavior: A social network perspective. *Academy of Management Review, 23,* 1 (1998), 14–31.

13. Bulgurcu, B.; Cavusoglu, H.; and Benbasat I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34,* 3 (2010), 523–548.

14. Churchill, G.A. A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research, 16,* 1 (1979), 64–73.

15. Conger, J.A., and Kanungo, R.N. The empowerment process: Integrating theory and practice. *Academy of Management Review, 13,* 3 (1988), 471–482.

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

17. Das, T.K., and Teng, B.-S. Between trust and control: Developing confidence in partner cooperation in alliances. *Academy of Management Review, 23,* 3 (1998), 491–512.

18. Dhillon, G., and Backhouse, J. Information system security management in the new millennium. *Communications of the ACM, 43,* 7 (2000), 125–128.

19. Edwards, W. Reward probability, amount, and information as determiners of sequential two-alternative decisions. *Journal of Experimental Psychology, 52,* 3 (1956), 177–188.

20. Eisenberger, R., and Cameron, J. Detrimental effects of reward: Reality or myth? *American Psychologist, 51,* 11 (1996), 1153–1166.

21. Eisenhardt, K.M. Control: Organizational and economic approaches. *Management Science, 31,* 2 (1985), 134–149.

22. Etzioni, A. *A Comparative Analysis of Complex Organizations: On Power, Involvement, and Their Correlates.* New York: Free Press, 1975.

23. Evans, M.G. A Monte Carlo study of the effects of correlated method variance in moderated multiple regression analysis. *Organizational Behavior and Human Decision Processes, 36,* 3 (1985), 305–323.

24. Fehr, E., and Schmidt, K.M. Adding a stick to the carrot? The interaction of bonuses and fines. *American Economic Review, 97,* 2 (2007), 177–181.

25. Finch, J. Research note: The vignette technique in survey research. *Sociology, 21,* 2 (1987), 105–114.

26. Fisher, R.J., and Ackerman, D. The effects of recognition and group need on volunteerism: A social norm perspective. *Journal of Consumer Research, 25,* 3 (1998), 262–275.

27. Fritzen, S.A. Crafting performance measurement systems to reduce corruption risks in complex organizations: The case of the World Bank. *Measuring Business Excellence, 1,* 4 (2007), 23–32.

28. Gerhart, B., and Milkovich, G.T. Organizational differences in managerial compensation and financial performance. *Academy of Management Journal, 33,* 4 (1990), 663–691.

29. Gewald, H.; Wüllenweber, K.; and Weitzel, T. The influence of perceived risks on banking managers' intention to outsource business processes: A study of German banking and finance industry. *Journal of Electronic Commerce Research, 7,* 2 (2006), 78–96.

30. Gordon, L.; Loeb, M.; Lucyshyn, W.; and Richardson, R. CSI/FBI computer crime and security survey, Computer Security Institute, San Francisco, 2006.

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

32. Greitemeyer, T., and Weiner, B. Asymmetrical effects of reward and punishment on attributions of morality. *Journal of Social Psychology, 148,* 4 (2008), 407–420.

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

34. Information security breaches survey 2008. BERR, UK Department for Business, Enterprise and Regulatory Reform, London, 2008 (available at www.bis.gov.uk/files/file45714.pdf).

35. Information security policy templates. SANS, Bethesda, MD, 2010 (available at www.sans.org/security-resources/policies/).

36. Jasso, G. Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research, 34,* 3 (2006), 334–423.

37. Keil, M.; Tan, B.; Wei, K.; Saarinen T.; Tuunainen, V.; and Wassenaar, A. A cross-cultural study on escalation of commitment behavior in software projects. *MIS Quarterly, 24,* 2 (2000), 299–325.

38. Kirsch, L.J. Portfolios of control modes and IS project management. *Information Systems Research, 8,* 3 (1997), 215–239.

39. Knapp, K.J.; Marshall, T.E.; Rainer, R.K.; and Ford, F.N. Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14,* 1 (2006), 24–36.

40. Kohn, A. Why incentive plans cannot work. *Harvard Business Review, 71,* 5 (1993), 54–62.

41. Leonard, L.N.K., and Cronan, T.P. Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association for Information Systems, 1,* 1 (2000), 1–31.

42. Leonard, L.N.K.; Cronan, T.P.; and Kreie, J. Situational influences on ethical decision-making in an IT context. *Information & Management, 44,* 3 (2007), 313–320.

43. Levinthal, D. A survey of agency models of organizations. *Journal of Economic Behavior & Organization, 9,* 2 (1988), 153–185.

44. Loch, K.D.; Carr, H.H.; and Warkentin, M.E. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16,* 2 (1992), 173–186.

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

46. Molm, L.D. Is punishment effective? Coercive strategy in social exchange. *Social Psychology Quarterly, 57,* 2 (1994), 75–94.

47. Moores, T., and Chang, J. Ethical decision making in software piracy: Initial development and a test of a four-component model. *MIS Quarterly, 30,* 1 (2006), 167–180.

48. Myyry, L.; Siponen, M.; Pahnila, S.; Vartiainen, T.; and Vance, A. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18,* 2 (2009), 126–139.

49. Nicholson, N. Ethics in organizations: A framework for theory and research. *Journal of Business Ethics, 13,* 8 (1994), 581–596.

50. Nunnally, J.C. *Psychometric Theory.* New York: McGraw-Hill, 1978.

51. Pahnila, S.; Siponen, M.; and Mahmood, A. Employees' behavior towards IS security policy compliance. In R.H. Sprague (ed.), *Proceedings of the 40th Annual Hawaii International*

Conference on System Sciences. Los Alamitos, CA: IEEE Computer Society Press, 2007, pp. 156–166.

52. Pavlou, P.A., and Fygenson, M. Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly, 30,* 1 (2006), 115–143.

53. Peace, A.G.; Galletta, D.F.; and Thong, J.Y.L. Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20,* 1 (Summer 2003), 153–177.

54. Pfeffer, J., and Salancik, G.R. *The External Control of Organizations: A Resource Dependence Perspective.* New York: Harper & Row, 1978.

55. Porter, L.W., and Lawler, E.E. *Managerial Attitudes and Performance.* Homewood, IL: Irwin-Dorsey, 1968.

56. Richardson, R. CSI computer crime & security survey. Computer Security Institute, San Francisco, 2008.

57. Ryan, M.J. Behavioral intention formation: The interdependency of attitudinal and social influence variables. *Journal of Consumer Research, 9,* 3 (1982), 263–278.

58. Ryan, R.M., and Deci, E. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist, 55,* 1 (2000), 68–78.

59. Sims, H.P., Jr. Further thoughts on punishment in organizations. *Academy of Management Review, 5,* 1 (1980), 133–138.

60. Siponen, M.T. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8,* 1 (2000), 31–41.

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

62. Sisaye, S. Teams and management control systems: A synthesis of three organizational development approaches. *Leadership & Organization Development Journal, 26,* 3 (2005), 172–185.

63. Smith, H.; Keil, M.; and Depledge, G. Keeping mum as the project goes under: Toward an explanatory model. *Journal of Management Information Systems, 18,* 2 (Fall 2001), 189–227.

64. Straub, D. Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14,* 1 (1990), 45–60.

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

66. Straub, D., and Welke, R. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22,* 4 (1998), 441–469.

67. Sussmann, M., and Vecchio, R.P. A social influence interpretation of worker motivation. *Academy of Management Review, 7,* 2 (1982), 177–186.

68. Taylor, S., and Todd, P. Assessing IT usage: The role of prior experience. *MIS Quarterly, 19,* 4 (1995), 561–570.

69. Tiwana, A., and Bush, A. A comparison of transaction cost, agency and knowledge-based predictors of IT outsourcing. *Journal of Management Information Systems, 24,* 1 (Summer 2007), 259–300.

70. Trevino, L.K. The social effects of punishment in organizations: A justice perspective. *Academy of Management Review, 17,* 4 (1992), 647–676.

71. Trevino, L.K.; Weaver, G.R.; Gibson, D.G.; and Toffler, B.L. Managing ethics and legal compliance: What works and what hurts. *California Management Review, 41,* 2 (1999), 131–151.

72. The 2008 insider threat survey: Workers admit to everyday behavior that puts sensitive business information at risk. White paper, RSA, Bedford, MA, 2008 (available at www.rsa.com/company/news/releases/pdfs/RSA_2008_Insider_Threat_Survey_WP.pdf).

73. Venkatesh, V.; Morris, M.; Davis, G.; and Davis, F. User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27,* 3 (2003), 425–478.

74. Vroom, V.H. *Work and Motivation.* New York: Wiley, 1964.

75. Wason, K.; Polonsky, M.; and Hyman, M. Designing vignette studies in marketing. *Australasian Marketing Journal, 10,* 3 (2003), 41–58.

76. Weber, J. Scenarios in business ethics research: Review, critical assessment, and recommendations. *Business Ethics Quarterly, 2,* 2 (1992), 137–160.

77. Zenger, T.R. Why do employers only reward extreme performance? Examining the relationships among performance pay and turnover. *Administrative Science Quarterly, 37,* 2 (1992), 198–219.

Appendix: Scenarios and Instrument

The descriptive text and the password and e-mail use policy presented to the experiment participants before the scenarios can be obtained from the authors upon request.

High Certainty Scenario 1 (High Certainty, Low Reward, Mild Punishment)

Mike is an employee of iCorp. He is aware that to enforce compliance of security policy, iCorp has its IT department monitor and record security policy compliance and violations by using the monitoring software on a regular basis. The CIO [chief information officer] and other departments get reports on security policy compliance and violations from the IT department annually. Each department holds a routine meeting at the end of the year. During the meeting, those who *had complied* with the security policies will be orally commended while those who *had violated* will be orally censured.

High Certainty Scenario 2 (High Certainty, Low Reward, Severe Punishment)

Mike is an employee of iCorp. He is aware that to enforce compliance of security policy, iCorp has its IT department monitor and record security policy compliance and violations by using the monitoring software on a regular basis. The CIO and other departments get reports on security policy compliance and violations from the IT department annually. Each department holds a routine meeting at the end of the year. During this meeting, those who *had complied* with the security policies will be orally praised while those who *had violated* will be orally censured and have *1 to 5 points deducted* from their merits (100-point base) based on the severity of the violations. These merit points directly link to their annual bonus that is added to their salary. These merit points also have implicit influences on promotion and other benefits.

High Certainty Scenario 3 (High Certainty, High Reward, Mild Punishment)

Mike is an employee of iCorp. He is aware that to enforce compliance of security policy, iCorp has its IT department monitor and record security policy compliance and violations by using the monitoring software on a regular basis. The CIO and other departments get reports on security policy compliance and violations from the IT department annually. Each department holds a routine meeting at the end of the year. During the meeting, those who *had complied* with the security policies will be orally praised and have *1 to 5 points added* to their merits (100-point base) based on the degree of compliance while those who *had violated* the security policies will be orally censured. These merit points directly link to their annual bonus that is added to their salary. These merit points also have implicit influences on promotion and other benefits.

High Certainty Scenario 4 (High Certainty, High Reward, Severe Punishment)

Mike is an employee of iCorp. He is aware that to enforce compliance of security policy, iCorp has its IT department monitor and record security policy compliance and violations by using the monitoring software on a regular basis. The CIO and other departments get reports on security policy compliance and violations from the IT department annually. Each department holds a routine meeting at the end of the year. During this meeting, those who *had complied* with will be orally commended and have *1 to 5 points added* to their merits (100-point base) based on the degree of compliance while those who *had violated* the security policies will be orally censured and have *1 to 5 points deducted* from their merits based on the severity of violations. These merit points directly link to their annual bonus that is added to their salary. These merit points also have implicit influences on promotion and other benefits.

Low Certainty Scenario 1 (Low Certainty, Low Reward, Mild Punishment)

Mike is an employee of iCorp. He knows that in the past, on average, iCorp had assessed its employees' security policy compliance and violations every other year. Those assessments were unscheduled. After each assessment, those who *had complied* with the security policies were orally commended while those who *had violated* were orally censured in their year-end departmental meeting.

Low Certainty Scenario 2 (Low Certainty, Low Reward, Severe Punishment)

Mike is an employee of iCorp. He knows that in the past, on average, iCorp had assessed its employees' security policy compliance and violations every other year. Those assessments were unscheduled. After each assessment, those who had complied with the security policies were orally commended while those who *had violated* were orally censured and have *1 to 5 points deducted* from their merits (100-point base) based on the severity of violations. These merit points directly link to their annual bonus that is added to their salary. These merit points also have implicit influences on promotion and other benefits.

Low Certainty Scenario 3 (Low Certainty, High Reward, Mild Punishment)

Mike is an employee of iCorp. He knows that in the past, on average, iCorp had assessed its employees' security policy compliance and violations every other year. Those assessments were unscheduled. After each assessment, those who *had complied* with the security policies were orally commended and have *1 to 5 points added* to their merits (100-point base) based on the degree of compliance while those who *had violated* were orally censured. These merit points directly link to their annual bonus that is added to their salary. These merit points also have implicit influences on promotion and other benefits.

Low Certainty Scenario 4 (Low Certainty, High Reward, Severe Punishment)

Mike is an employee of iCorp. He knows that in the past, on average, iCorp had assessed its employees' security policy compliance and violations every other year. Those assessments were unscheduled. After each assessment, those who *had complied* with the security policies were orally commended and have *1 to 5 points added* to their merits (100-point base) based on the degree of compliance while those who *had violated* got orally censured and have *1 to 5 points deducted* from their merits based the severity of violations. These merit points directly link to their annual bonus that is added to their salary. These merit points also have implicit influences on promotion and other benefits.

Given this hypothetical scenario and assuming you were Mike, please specify the extent to which you would agree or disagree with the following statements (7-point scales: 1 = "strongly disagree," 7 = "strongly agree") (items were adapted from [16, 39, 73]. This part of the text and questions were repeated for each of the four scenarios presented to each participant):

1. It is possible that I will follow iCorp's security policies. (*Compliance_Intent1* or *CI1*)
2. It is probable that I will follow iCorp's security policies. (*CI2*)
3. I am likely to follow iCorp's security policies. (*CI3*)
4. I am certain that I will follow iCorp's security policies. (*CI4*)*
5. If I violate iCorp's security policies, the chance I would be caught is high. (*ManiCheck_Perceived_Certainty 1* or *MANI-C1*)
6. If I were caught violating iCorp's security policies, I would be punished severely. (*ManiCheck_Perceived_Punishment_Severity* or *MANI-P*)
7. If I follow iCorp's security policies, the chance I would get rewarded is high. (*ManiCheck_Perceived_Certainty 2* or *MANI-C2*)
8. If I follow iCorp's security policies, I would be rewarded greatly. (*Mani_Check_Perceived_Reward_Significance* or *MANI-R*)

After completing the above (four) scenarios and the corresponding questions related to each scenario, respondents answered the following questions that are related to *their own current organization, not* to iCorp.

1. Employees in my organization value the importance of security of information and computer systems. (*Security_Culture1* or *SC1*)
2. In my organization, a culture exists that promotes good security and privacy practices. (*SC2*)
3. Security (of information and systems) has traditionally been considered an important organization value. (*SC3*)
4. Practicing good security of information and computer systems is the accepted way of doing business in my organization. (*SC4*)
5. The overall environment in my organization fosters security-minded thinking in all our actions. (*SC5*)
6. Information and systems security is a key norm shared by all organizational members/employees. (*SC6*)
7. Protecting customer, internal employee, and other trading partner information is very important in my organization. (*SC7*)
8. The information I deal with in my daily work is such that it is imperative to ensure confidentiality and maintain privacy. (*SC8*)
9. To accomplish their work, employees are willing to take risks of not complying with information and systems use guidelines. (SC*9*)*
10. My organization has specific guidelines that describe acceptable use of e-mail. (*Security_Policy1* or *SP1*)
11. My organization has established rules of behaviors for use of computer recourses. (*SP2*)
12. My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use. (*SP3*)
13. My organization has specific guidelines that describe acceptable use of computer passwords. (*SP4*)*
14. My organization has specific guidelines that govern what employees are allowed to do with their computers. (*SP5*)
15. My organization provides training to help employees improve their awareness of computer and information security issues. (*Security_Training1* or *ST1*)*
16. My organization provides employees with education on computer software copyright laws. (*ST2*)
17. In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way. (*ST3*)
18. My organization educates employees on their computer security responsibilities. (*ST4*)
19. In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use. (*ST5*)
20. I believe that my organization monitors any modification or altering of computerized data by employees. (*Security_Monitoring1* or *SM1*)

21. I believe that employee computing activities are monitored by my organization. (*SM2*)
22. I believe that my organization monitors computing activities to ensure that employees are performing only explicitly authorized tasks. (*SM3*)
23. I believe that my organization reviews logs of employee computing activities on a regular basis (*SM4*)
24. I believe that my organization conducts periodic audits to detect the use of authorized software on its computers. (*SM5*)
25. I believe that my organization actively monitors the content of employees' e-mail messages. (*SM6*)

* Item dropped during the scale refinement (factor analyses) process.