11-2019
Working Paper Number 19024

Information Security Policy Compliance

Yuanxiang John Li
Iowa State University

Elizabeth Hoffman
Iowa State University, bhoffman@iastate.edu

Information Security Policy Compliance

Abstract

One of the most challenging problems modern firms face is that their weakest link in maintaining information security is the behavior of employees: clicking on phishing emails, telling friends and family private information, and searching for private information about themselves (Loch, Carr and Warkentin 1992). A survey conducted by the Computer Security Institute reported that the average monetary loss per incident was $288,618 and that 44% of those who responded to the survey reported insider security-related abuse, making it the second-most frequently occurring computer security incident (Richardson 2008).

This paper uses a questionnaire from Hu, West and Smarandescu (2015) to test for the efficacy of different reward and punishment schemes in preventing insider security-related abuse. Hu et al.'s (2015) scenarios elicit from participants whether they would recommend violating company IT policies. Real monetary payments provide motivation.3 The results indicate that, if a company can detect abuses with some degree of certainty, the best strategy among those tested is to regularly reward individual employees with small rewards for complying with company policy and punish every detected violation. This recommendation contrasts with the existing literature, which focuses almost entirely on punishment for detected security breaches. This focus on punishment is referred to as General Deterrence Theory (Straub Jr 1990). The results in this paper suggest strongly that General Deterrence Theory does not provide an effective strategy for preventing security breaches.

Disciplines

Behavioral Economics | Economic Theory

Information Security Policy Compliance*

November 2019

Yuanxiang John Li[1] and Elizabeth Hoffman[2]

Abstract

One of the most challenging problems modern firms face is that their weakest link in maintaining information security is the behavior of employees: clicking on phishing emails, telling friends and family private information, and searching for private information about themselves (Loch, Carr and Warkentin 1992). A survey conducted by the Computer Security Institute reported that the average monetary loss per incident was $288,618 and that 44% of those who responded to the survey reported insider security-related abuse, making it the second-most frequently occurring computer security incident (Richardson 2008).

This paper uses a questionnaire from Hu, West and Smarandescu (2015) to test for the efficacy of different reward and punishment schemes in preventing insider security-related abuse. Hu et al.'s (2015) scenarios elicit from participants whether they would recommend violating company IT policies. Real monetary payments provide motivation.[3] The results indicate that, if a company can detect abuses with some degree of certainty, the best strategy among those tested is to regularly reward individual employees with small rewards for complying with company policy and punish every detected violation. This recommendation contrasts with the existing literature, which focuses almost entirely on punishment for detected security breaches. This focus on punishment is referred to as General Deterrence Theory (Straub Jr 1990). The results in this paper suggest strongly that General Deterrence Theory does not provide an effective strategy for preventing security breaches.

*The authors would like to thank the participants at the Economic Science Association Annual Meetings in San Diego in 2017, professors James Davis and Dan Zhu at Iowa State University, the other graduate students in Professor Hoffman's experimental/behavioral classes, and Brian Binger for extensive editorial comments. All errors remain our own.

[1] Visiting Scholar, Iowa State University, Ames, Iowa 50011 (yxli@iastate.edu)

[2] Professor of Economics, Iowa State University, Ames, Iowa 50011 (bhoffman@iastate.edu)

[3] There is considerable experimental economics literature showing that monetary incentives are more effective than surveys to generate reliable responses. (See, for example, Binger et al., 1995; Hoffman and Spitzer, 1993; and Shogren et al., 1994).

1. Introduction

One of the most challenging problems modern firms face is that their weakest link in maintaining information security is the behavior of employees: clicking on phishing emails, telling friends and family private information, and searching for private information about themselves (Loch, Carr and Warkentin 1992). A survey conducted by the Computer Security Institute reported that the average monetary loss per incident was $288,618 and that 44% of those who responded to the survey reported insider security-related abuse, making it the second-most frequently occurring computer security incident (Richardson 2008).

Given the integral role of IT in today's enterprises, information security must be a key component in modern enterprise planning and management (Chang and Ho 2006). Information security refers to the extent to which corporate information is free from disclosure, modification, or destruction due to intentional or unauthorized access (Finne 2000). In order to protect against security breaches, organizations often rely on technology-based solutions (Ernst and Young 2008, PwC 2008).

However, technology cannot guarantee information security without a good management policy that is properly implemented. Moreover, information security is not exclusively a technical problem but also a behavioral issue (Dhillon and Backhouse 2000, Dutta and McCrohan 2002, So and Sculli 2002, Vermeulen and Von Solms 2002, Von Solms and Von Solms 2004). Success in information security can be achieved when organizations invest both in technical solutions and in incentives to improve employees' compliance with information security policies (Bulgurcu, Cavusoglu and Benbasat 2010).

It has long been recognized that companies' information security efforts are threatened by employee negligence and insider breaches (Loch, Carr and Warkentin 1992). Employees are often the weakest link in maintaining information security (Mitnick and Simon 2002, Warkentin and Willison 2009). There is a large body of MIS literature, based on General Deterrence Theory (Straub Jr 1990) discussing how to "punish" employees if they do not comply with the information security policy in a firm. On the other hand, some recommendations take a "gentler" approach, such as using rewards or incentives, to reduce their employees' noncompliance (Bulgurcu, Cavusoglu and Benbasat 2010, Padayachee 2012, Pahnila, Siponen and Mahmood 2007, Vance and Siponen 2012). However, few papers incorporate both means to reduce information security breaches (Chen, Ramamurthy and Wen 2012, Liang, Xue and Wu 2013).

To the best of our knowledge, no extant MIS literature has used experiments with human subjects and monetary incentives to examine employees' compliance behaviors (See Smith 1976, for a discussion of the use of monetary incentives in experiments using human subjects). A Sommestad et al. (2014) review paper examined 29 studies with more than 60 possible variables hypothesized to improve information security policy compliance and deter noncompliance. No dominant variables were clearly identified. Most of these studies measure improvement or deterrence through a self-reported survey or a hypothetical single-scenario-based experiment without real incentives paid to participants; hence, there is reason to believe that using many different scenarios and real economic incentives will further the understanding of how reward

and punishment influence employees' behavior with regard to complying with a firm's information security policy.

From an organization's perspective, rewards and punishments are two very practical ways for a company to motivate its workforce to reduce security breaches. A meta-analysis done by Balliet, Mulder and Van Lange (2011) revealed that both rewards and punishments had a medium to large effect on IT policy compliance. In the IT world, a security violation is different from a regular policy violation in the non-IT world. A single data breach caused by even one employee can lead to negative effects on the whole organization.

This paper also considers the impact of collective rewards and punishments. Although modern western companies do not employ collective rewards or collective punishments, they were commonly used in U.S. military boot camps in the 1980s (Gilham 1982). Heckathorn (1988) showed that when leaders use collective rewards and punishments to encourage compliance group members monitor and regulate one another's behavior.

This study may also be the first to analyze the impact of collective rewards and collective punishments on information security compliance. This paper aims to assist organizations in designing a realistic and effective managerial policy and payment structure to prevent data breaches. Specifically, this paper considers the following research questions:

> RQ1: How do monetary rewards affect employees' compliance with an information security policy?
> RQ2: How do monetary punishments affect employees' compliance with an information security policy?
> RQ3: What are the combined effects of monetary rewards and punishments on employees' compliance with an information security policy?
> RQ4: Does the implementation of collective rewards or punishments affect employees' compliance with an information security policy?
> RQ5: How do changes in the probability of being detected by a monitoring system affect employees' compliance with an information security policy when there is a fairly low probability of being detected as not complying?

The rest of the paper is organized as follows. Section 2 reviews previous work on compliance in the information security literature. Section 3 develops the core hypotheses. Section 4 outlines the research methodology. Section 5 presents the data collection and analyses. Sections 6 and 7 present and discuss the results. Section 8 presents the conclusions and elaborates on their implications and limitations, suggesting further research. The appendices present some of the econometric analyses, the scenarios, and the instructions.

2 Review of the Literature

2.1. Human Factors in Information Security

The insider threat is always present and manifests itself in many ways in human society (Colwill 2009). The Target security breach in 2013 (Abrams 2014, Rockefeller 2014, Wallace 2014) illustrates the severe consequence of employees' noncompliant behavior. According to the report from the Committee on Commerce, Science, and Transportation (Rockefeller 2014), Target's payment network system was intruded via its third-party vendor, Fazio Mechanical Services, a provider of refrigeration and HVAC systems. Some employees' virtual private network credentials were stolen through a phishing attack of malware delivered in an email at Fazio. Hackers then used the stolen credential information from Fazio to remotely log into Target's network payment system, stealing the payment and personal information of as many as 110 million customers, and then copied this sensitive information from Target's network to a server in Eastern Europe.

This particular breach affected more than a third of the U.S. population, exposing 34% of Americans' financial information (Wallace 2014). This massive data breach directly led to a more than $148 million dollar loss to Target's shareholders (Abrams 2014). Furthermore, in order to maintain loyal customers, Target has been providing free credit monitoring for its customers, further undermining Target's profitability. Moreover, Target faces lawsuits from its customers, imposing additional costs on the company.

Even in governmental organizations, insiders are prone to information security failures (Colwill 2009). The UK Government's Revenue and Customers Department lost the personal information of 25 million people in a single incident (Thomson 2007). Research shows that insiders, not outsiders, are responsible for 70% of data breaches; however, organizations focus 90% of security controls and monitoring on external threats (McCue 2008).

The Datalossdb Open Security Foundation website shows that about 24% of the total data-loss incidents in 2012 were due to employees violating organizational IT policies. In addition, the ongoing PwC survey in the UK in 2015 shows that 75% of information security breaches in large organizations were the result of human factors. This figure is an increase from 58% one year earlier (PwC 2015). Similarly, the Chronology of Data Breaches shows that in 2012 in the U.S., approximately 9,232,015 records were stolen as the result of insider data breaches. The Ponemon Institute shows that 35% of data breaches around the world were due to human errors (Alaskar, Vodanovich and Shen 2015).

Although external hackers are sophisticated, with advanced technology skills, much research (Bulgurcu, Cavusoglu and Benbasat 2010, Herath and Rao 2009, Hu et al. 2012, Hu et al. 2011, Myyry et al. 2009, Warkentin and Willison 2009) has shown that the human agent is still the weakest link in the defense against threats to organizational information assets. Nevertheless, no information security practice or technique is effective if not properly followed by employees (Ernst and Young 2002, Puhakainen 2006).

However, the responsibility for following organizational security policies is typically delegated to employees (Herath and Rao 2009). Employees may leak the organization's information assets for their own benefits or simply ignore the security policy (Puhakainen 2006). As a result, there is a conflict between employees' interests and those of the organization.

In order to motivate employees to comply with an organization's information security policy, the organization tries to "induce" employees to behave as it intends to by aligning both entities' interests. For example, if the organization could reliably monitor employee behavior, it could pay a regular bonus on top of each employee's base salary to those employees who regularly comply with the organization's information security policy. Essentially, the paid bonus could reconcile the conflict between employees' noncompliance with the organization's security requirement and the organization's need for compliance. Paying bonuses to employees who regularly comply could be combined with fining employees who are detected as not complying with the organization's information security policies. Such a combined policy of rewards and punishments might further enhance employees' compliance.

Despite the possible advantage of combining rewards and punishments, neither managerial academic literature nor industry practice emphasizes this incentive structure in information security compliance. Organizations rely on the perceived force of regulation (e.g., sanctions) and believe it is each employee's duty to obey the rules.

2.2. Employees Compliance with an Organization's Information Security Policies

An information security policy violation can be very serious for an organization, as the consequence of one non-compliant action can compromise an organization's entire information security system. As illustrated by the Target breach, one employee's noncompliance can be very costly for the organization. The ideal situation for an organization is that all its employees should comply with the organization's information security policy. However, one non-compliant employee may be difficult to detect. This paper studies detection and incentives in reducing employee non-compliance with information security policies.

Biological and social science research has shown that incentives are powerful means to align individual and group interests (Edney and Harper 1978, Fehr and Gächter 2000, Hashim and Bockstedt 2015, Henrich 2006, Lynn and Oldenquist 1986, Ostrom, Walker and Gardner 1992, Rand et al. 2009, Sigmund 2007, Yamagishi 1986). As the organization wants its employees to comply with its information security policy, providing positive incentives for compliance and negative sanctions for non-compliance will encourage each individual employee to conform to the organization's information security policy.

To summarize, the information security of an organization is not merely dependent on its hardware-software sophistication, nor on some employees' good behavior, but also on all employees' compliance with the organization's information security policies. The ability to detect data breaches may be as important as the incentives employed to increase compliance. One of the questions this paper asks is: can an organization significantly improve compliance with a combination of rewards and punishments? Moreover, does it matter if detection is certain or uncertain?

3 Theoretical Arguments and Core Hypotheses

3.1. General Deterrence Theory

According to the review paper by Alaskar, Vodanovich and Shen (2015), General Deterrence Theory is still the dominant theory used by Information Systems scholars to study information security compliance (Chen, Ramamurthy and Wen 2012, Cheng et al. 2013, D'Arcy, Hovav and Galletta 2009, D'Arcy and Hovav 2009, Guo and Yuan 2012, Harrington 1996, Herath and Rao 2009, Herath and Rao 2009, Lee, Lee and Yoo 2004, Siponen and Vance 2010, Son 2011, Straub Jr 1990). Straub Jr and Nance (1990) adopted classical deterrence theory from criminology literature into their information security studies. Deterrence theory posits that individuals weigh costs and benefits when deciding whether or not to engage in criminal behavior (Siponen and Vance 2010). This is similar to the economic argument by Becker (1968) and Becker (1974) on the economic theory of criminal behavior.

In the information security setting, Straub Jr (1990) argues that violation behavior can be reduced by imposing sanctions that are certain and severe to potential rule-breakers. However, another review paper by Sommestad et al. (2014) concludes that general deterrence theory has questionable efficacy. The perceived severity of sanctions and the perceived certainty of sanctions have limited power over employees' noncompliance behavior. Hence, deterrence alone will not significantly reduce information breaches.

3.2. Detection and Incentives

As noted above, current MIS literature tends to focus mostly on punishments and occasionally on rewards, but not on both at the same time. The MIS literature does not address problems associated with an inability to reliably detect employee behavior. Moreover, the current literature focuses heavily on surveying participants for their compliance intentions, rather than on providing actual monetary incentives for compliant behavior or monetary disincentives for noncompliant behavior. This study starts with the assumption that a company can reliably detect both compliance and noncompliance. It tests for the importance of this assumption later. Use of monetary incentives and the assumption of reliability of detection lead to the following hypotheses.

> *H1: Monetary Rewards for compliance will have a positive impact on employees' compliance with a company's information security policy.*
>
> *H2: Monetary Punishments for noncompliance will have a positive impact on employees' compliance with a company's information security policy.*
>
> *H3: Monetary Rewards for compliance and monetary punishment for noncompliance together will have stronger positive impacts on employees' behavior in complying with a company's information security policy when compared with either a monetary reward only or a monetary punishment only policy.*

3.3. Collective Sanctions

Collective sanctions is a system such that rewards or punishments extend not only to the actors but to the actors' groups (Heckathorn 1990). In such systems, when an individual violates or complies with a rule, not merely the individual, but all other members of that person's group as well, are collectively rewarded or punished by an external agent (Heckathorn 1988). The literature summarized above assumes that individual rewards and punishments are two distinct and effective means to enhance compliance with an information security policy. However, a few noncompliant employees, rather than the compliant majority, determine the level of a company's information security defense. The goal for an organization is to eliminate noncompliance.

Modern organizations rarely use collective sanctions. However, they are commonly used in U.S. military boot camps to enhance the effectiveness of control (Gilham 1982). A more extreme application of collective sanctions occurred in Stalinist prisons (Dallin and Nicolaevsky 1947), where prisoners earned points through work and compliance with prison rules and the distribution of food, medicine, and other essentials of life depended on the points earned by the group. The use of collective sanctions may not appeal to some employees, but an organization may improve compliance if the organization rewards all or punishes all when one or more employees is detected as complying, or not complying, with the organization's information security policy incentives. This payment structure might be more effective in maintaining compliance with an information security policy than traditional deterrence.

3.4. Complete and Incomplete Monitoring

As noted above, the treatments discussed thus far assume a company has complete information about employees' information security policy compliance. More realistically, a company usually relies on some sort of detection system (e.g., Intrusion Detection Systems) to monitor the input/output information traffic to detect abnormal activities. Khan, Awad and Thuraisingham (2007) shows that the detection accuracy rate could range from 11% to 95%. Even the best detection systems are never perfect in a real-world setting. In fact, research by computer scientists and computer engineers (Anderson, Frivold and Valdes 1995, Garcia-Teodoro et al. 2009, Ilgun, Kemmerer and Porras 1995, Kumar and Spafford 1995, Lee and Stolfo 2000, Lippmann et al. 2000, Porras and Neumann 1997, Sequeira and Zaki 2002, Stolfo et al. 2001, Yu, Yang and Han 2003) still cannot identify a definitive accuracy rate of an Intrusion Detection Systems.

In the context of information security policy compliance, a low chance of being caught could undermine the effect of rewards and punishments on employees' compliance with an information security policy. Boss et al. (2009) shows that if one knows he/she is being watched, he/she will follow the information security policy; otherwise, the rules will often be ignored. Accordingly, this study considers the following hypotheses,

> *H4: A reduction in the chance of being identified as not complying with an information security policy will have a negative impact on employees' level of compliance with that policy.*

H5: A reduction in the chance of being identified as not complying with an information security policy will reduce the positive effects of rewards for promoting employees' level of compliance with that policy.

H6: A reduction in the chance of being identified as not complying with an information security policy will reduce the positive effects of punishments for violating the policy.

4. Research Methodology

4.1. Scenario-based Security Compliance Measurement

The papers by Sommestad et al. (2014) and Alaskar, Vodanovich and Shen (2015) point out that the survey is the predominant research method used in the management of information security literature. However, it is well known that using self-reported data is biased, especially in studying anti-social and ethical/unethical behavior (Krumpal 2013). Scenario-based methods, which ask subjects to imagine themselves as someone else may be effective in reducing self-report bias (Pogarsky 2004). In the field of Information Systems, scenario methods have been widely used to study various topics in information security research. Myyry et al. (2009) use a single scenario to study the influence of being asked to think about moral responses on employees' compliance with information security policies. Cheng et al. (2013) also uses a single scenario test and develops an integrated model based on social control and deterrence theory to study information security policy violations. D'Arcy, Hovav and Galletta (2009), Barlow et al. (2013), and Hu, West and Smarandescu (2015) use multiple scenarios to observe employees' information compliance/noncompliance. Other papers randomly assign one scenario per participant (Chen, Ramamurthy and Wen 2012, D'Arcy and Hovav 2009, Guo and Yuan 2012, Guo et al. 2011, Harrington 1996, Hu et al. 2011, Vance and Siponen 2012).

The scenario method offers distinct advantages for research on unethical or socially undesirable behavior, especially when participants do not respond directly about themselves. Due to the secrecy involved in the undesirable behavior, individuals are more likely to conceal their real response to the questions and provide socially desirable answers to the researcher (Trevino 1992). However, a hypothetical scenario might make participants feel less reluctant to report their actual intentions when acting similarly to the person described in the scenario (Harrington 1996). Additionally, hypothetical scenarios drawn from experts could specify the situational details to enhance the realism of decision-making by providing contextual details (Alexander and Becker 1978). While the scenario method does not have the external validity of experimental studies using induced values (Smith 1976), it has been accepted in the managerial literature as an improvement compared to surveys asking subjects to report on their own (possibly) non-compliant behavior (Hu, West and Smarandescu 2015).

This research, adopts the multiple scenarios of minor and major violations developed by Hu, West and Smarandescu (2015). The scenario method also increases the generalizability of conclusions, as the large number of scenarios is more likely to capture some realistic situations. Each participant is instructed to imagine herself/himself as a hypothetical employee called "Josh" of a "company" and asked to answer a question posed in each of 30 scenarios as if the subject were Josh. Hu, West and Smarandescu (2015) categorized each situation as either a

major or a minor information security violation. This study adopted 15 minor and 15 major hypothetical scenarios.[4] Participants were presented with scenarios in a pseudorandom order (the order of the scenarios was randomized but consistent across all participants), omitting Hu et al.'s (2015) control group. This strategy allowed the elimination of the possible effect of having different subjects see the scenarios in different orders.

4.2. Real Dollar Incentives Compared to Hypothetical Incentives

The literature review indicates that hypothetical scenario-based methods are widely used in the Information Systems field for studying information security research; however, experimental subjects in the IS literature are rarely paid different amounts which depend on their responses. Accordingly, this paper adopts the experimental economics approach of paying participants real money for responding to differential incentive scenarios. This is a significant methodological contribution to the Information Systems literature, as a great deal of experimental economics research has shown that real dollars can completely change the results.

Regarding group-level cooperation, Balliet, Mulder and Van Lange (2011) meta-analysis shows that both rewards and punishments are more effective when participants are actually paid for their decisions rather than when they make hypothetical decisions without monetary consequence. Furthermore, incentives seem to matter more when the monetary stakes are greater (Balliet, Mulder and Van Lange 2011). An organization's practical problem in information security is to design a suitable and effective incentive structure to motivate employees to comply with the organization's policies. Balliet, Mulder and Van Lange (2011) paper further points out that real monetary incentives are more effective than hypothetical incentives. Hoffman and Spitzer (1993), Shogren et al. (1994), and Binger, Copple and Hoffman (1995) also illustrate the importance of monetary incentives in human behavior studies. The experimental economics approach should show how monetary rewards and punishments influence employees' compliance with an information security policy.

4.3. Research Design

There are four designs in this study. Design 1 is a basic 2x2 factorial design containing four groups of subjects. It evaluates the effect of individual rewards and individual punishments on compliance with an organization's information security policy. Subjects also know that not complying gives them personal benefits that depend on the severity of the infraction. In addition, we test if individual rewards and individual punishments together are not simply adding to one another, but rather have a super-additive effect. Design 2, with three groups of participants, introduces collective sanctions (including collective rewards and collective punishments) to compare with design 1. Design 2 explores how collective sanctions influence employees' compliance. Design 3, building upon design 1, uses the 2 x 2 factorial design, but there is only a 20% chance that any one subject will be detected as complying or not complying with an organization's information security policy. We consider how incomplete monitoring affects the degree to which subjects respond to the rewards, punishments, and personal benefits of non-

[4] Appendix A gives the scenarios in the order presented to our subjects.

compliance. Lastly, design 4, with three groups of subjects, includes both collective sanctions and 20% monitoring. Design 1 uses individual incentives, whereas designs 2-4 use group-based incentives. Each group of 5 participants is determined randomly. The group members are fixed without reshuffling through the entire session. Each session is composed with 30 aforementioned scenarios and no participants are allowed to take more than one session in our experiments.

Any choice of a particular set of rewards, punishments, and personal benefits is likely to affect the results. Thus, Design 1 is a starting point in studying the impact of monetary rewards and punishments on compliance with an information security policy. This study starts with a simple set of rewards, punishments, and personal benefits. Each participant starts with 500 endowment tokens (100 tokens = $1.3) to use in this study. If a participant chooses "yes" after reading any given scenario, the participant is indicating that if s/he were "Josh," s/he imagines s/he would engage in an activity that violates the company's information security policy in the situation described in the scenario. Answering "yes" gains a participant between 1 and 30 tokens, representing the personal benefits "Josh" gains from violating a company's information security policy. Tokens gained by answering "yes" to any specific scenario are randomly selected from a uniform distribution from 1-9 for minor violations and 11-30 for major violations. Hu, West and Smarandescu (2015) classified each of the 30 scenarios as minor or major. In the absence of more information, each participant can assume that the expected value of answering "yes" to any scenario is 12.75 tokens. To keep the rewards and punishments close in value to the personal benefits, this study uses 10 tokens as either a reward for "Josh's" compliance or a punishment for his non-noncompliance. The wording, specific order, and personal benefits of answering "yes" to each scenario is in Appendix A. The experimental instructions are in Appendix B. The instructions are as neutral as possible, referring to punishments and rewards simply as changes to participants' payoffs. Participants were able to keep track of their earnings in real time.

Table 1 illustrates the Expected Value of payoffs (i.e., tokens) to participants in Design 1.

Table 1 Design 1 Payoffs

	EV NO	**EV Yes**
No Rewards or Punishments	0	12.75
Rewards Only	10	12.75
Punishments Only	0	2.75
Both Rewards and Punishments	10	2.75

All experiments were conducted using the oTree environmental Platform, an open-source Python- and Django-based platform for laboratory, online and field experiments (Chen, Schonger and Wickens 2016). Table 2 presents an overview of the four designs with their 14 treatment groups (See Appendix C for the specific designs of the treatments).

Table 2 Design Overview

Design 1	Design 2	Design 3	Design 4
Exp1C: Control		**Exp3C**: Control with 20% Inspection	
Exp1R: Individual Reward (100% inspection)	**Exp2R**: Collective Reward (100% inspection)	**Exp3R**: Individual Reward with 20% Inspection	**Exp4R**: Collective Reward with 20% Inspection
Exp1P: Individual Punishment (100% inspection)	**Exp2P**: Collective Punishment (100% inspection)	**Exp3P**: Individual Punishment with 20% Inspection	**Exp4P**: Collective Punishment with 20% Inspection
Exp1RP: Individual Reward & Punishment (100% inspection)	**Exp2RP**: Collective Reward & Punishment (100% inspection)	**Exp3RP**: Individual Reward & Punishment with 20% Inspection	**Exp4PR**: Collective Reward & Punishment with 20% Inspection

5 Data Collection and Analysis

5.1. Experimental Subjects and Data Collection

Students at a major Midwestern U.S. university participated in this study. About half of the subjects were drawn from the business college subject pool and the rest of subjects were recruited from the general undergraduate population not in the business college. The questions included risk attitudes, impulsivity, age, gender, education, and other demographic variables. Siponen and Vance (2010) and Vance and Siponen (2012) considered differences in responses between students and information security professionals and did not find significant differences. They argue that students can be used as subjects to study compliance with information security policies.

In total, 285 business school students participated. Students who showed up at the appointed time received course credit and $10 on average to complete the study. Their final compensation depended on their task performance, which is incorporated in the designed treatments and was introduced in the Design section.

The second population was the general undergraduate students (about 24,000), excluding business majors. About 600 students signed up for the study and 360 students showed up at the study location. Those students who showed up received $5 for their participation, instead of the course credit given to the business students. All other incentive and experimental treatments remained the same as for the first population. No students from either population were permitted to participate in more than one design section.

The data collection from the first population was conducted from the end of September to mid-October, 2016. General students' data from the second population was collected from late October to mid-November. Each experimental session lasted about 45 minutes.

After consent forms were distributed, students were given whatever time they needed to read through and sign the forms. Then, they went through the first part of the study, which is the 30 scenario-based questions. To enhance the saliency of the treatment manipulation, the core instruction about what would "Josh" do was repeatedly displayed underneath each scenario when participants were making their decisions. Additionally, the answering options (i.e., "Yes" or "No") for each scenario were not displayed until 20 seconds had elapsed to enhance the treatment.

After students made their decisions for each scenario, a current summary of tokens earned was displayed. At the end, after all 30 scenarios, students were informed how much cash they would receive from the study. Then, after all students finished the first part of the study, they filled out an online survey to gather their demographic information, risk assessment, risk preference, impulsivity assessment, computer skills and so on (see Appendix D for details).

After all students finished their surveys, they were instructed to fill out the necessary paperwork for payment. Then, they were instructed to log off their computers to ensure their privacy and to receive their payment (concealed in an individual envelop).

5.2. Data-Analysis Procedure

Each question allowed only two choices, "Yes" or "No. "Yes" means advice that "Josh" should not comply; whereas, "No" means advice that "Josh" should comply with the information security policy. To control for the potential effect caused by the different wording of 30 scenarios, the treatment-effect data analysis was calculated as follows. First, the scenario-based compliance ratio for each of 14 treatment groups was calculated. The compliance ratio for each scenario in each treatment group is the proportion of participants who chose "No" divided by the total number of participants in that treatment group. For example, the compliance ratio for Scenario 1 in the Control group of Design 1 (Exp1C) is 0.714286, since 35 out of 49 subjects chose "No" in this treatment group.

Second, the pair-wise difference of compliance ratio (DCR) between each of the 14 treatment groups was calculated. This was done to control for the potential effects of 30 differently worded scenarios. For example, the compliance ratio of Exp1R for Scenario 1 is 0.808511. Hence, the DCR between Exp1R and Exp1C is 0.094225 for Scenario 1. This is the individual Reward treatment effect (without the confounding caused by scenario wording) compared with the basic control group. Third, a time series data analysis was conducted to test if the series (i.e., 30 scenarios) of DCR numbers are not equal to zero. Particularly, an autoregressive model[5] with AR=1 was employed because each treatment group's current decision might be correlated to its previous decision through the 30-repeated observations (i.e., 30 scenario questions), as each subject was shown the scenario questions in the same order. Finally, the t-statistic and p-value of the constant term in the time-series data analysis were calculated to determine if the respective treatment had an effect.

[5] ARIMA model with orders of (1,0,0), (1,0,1), (1,0,2), (2,0,1), and (2,0,2) were also tested for each series of DCR to obtain the best fitting models by AIC index. For the sake of model concise and parsimonious, an AR=1 autoregressive model was adapted to report in this paper, as essentially the best fitting models provide the same data-analysis results. The ARIMA data-analysis results will be provided upon request.

In addition, a logistic regression with dummy codes to control for scenario differences, using the number of "No" answers by each individual as the dependent variable, was estimated. This regression tested whether participants' demographic and other control variables impacted their decisions to choose "No".

6. Experimental Results and Discussions

The overall experimental results are summarized in Table 3. It shows the coefficient and p-value of the constant term of the autoregressive model for all DCR combinations. The complete output of the AR=1 model is attached in Appendix E. In our time series data analysis, the constant term represents the estimated difference of two means between their respective treatment groups. For example, the estimated difference between Exp3C and Exp1C is -0.038 with a p-value as 0.015, which indicates that a low chance of being detected has a significantly negative impact on information security compliance compared with the most basic control group (1C).

Table 3 Experimental Results Overview

Mean.diff & p-value	Exp1 P	Exp1 R	Exp1R P	Exp2 P	Exp2 R	Exp2R P	Exp3 C	Exp3 P	Exp3 R	Exp3R P	Exp4 P	Exp4 R	Exp4R P
Exp1C	0.026	0.101	0.193	-0.091	-0.150	0.016	-0.038	-0.087	0.035	0.022	-0.123	0.063	0.057
	0.210	0.000	0.000	0.000	0.000	0.465	0.015	0.003	0.213	0.369	0.000	0.000	0.018
Exp1P		0.074	0.167	-0.118	-0.179	-0.014	-0.063	-0.117	0.005	-0.008	-0.150	0.036	0.028
		0.000	0.000	0.000	0.000	0.635	0.000	0.000	0.877	0.777	0.000	0.131	0.268
Exp1R			0.093	-0.192	-0.252	-0.087	-0.138	-0.191	-0.069	-0.083	-0.224	-0.039	-0.046
			0.000	0.000	0.000	0.003	0.000	0.000	0.043	0.004	0.000	0.121	0.066
Exp1RP				-0.285	-0.345	-0.180	-0.231	-0.283	-0.162	-0.175	-0.317	-0.131	-0.139
				0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Exp2P					-0.060	0.106	0.053	0.002	0.124	0.112	-0.032	0.156	0.149
					0.000	0.000	0.001	0.904	0.000	0.000	0.004	0.000	0.000
Exp2R						0.168	0.110	0.064	0.187	0.174	0.028	0.215	0.211
						0.000	0.000	0.000	0.000	0.000	0.060	0.000	0.000
Exp2RP							-0.054	-0.103	0.020	0.006	-0.139	0.048	0.041
							0.034	0.000	0.220	0.702	0.000	0.006	0.037
Exp3C								-0.050	0.072	0.059	-0.085	0.101	0.095
								0.121	0.031	0.011	0.000	0.000	0.000
Exp3P									0.123	0.110	-0.035	0.151	0.146
									0.000	0.000	0.012	0.000	0.000
Exp3R										-0.013	-0.158	0.029	0.022
										0.452	0.000	0.114	0.249
Exp3RP											-0.146	0.041	0.037
											0.000	0.002	0.000
Exp4P												0.188	0.183

		0.000	0.000
Exp4R			-0.005 0.733

6.1. Design 1 Results and Discussion

Design 1 was conducted to identify how individual reward and punishment with 100% detection, influenced employees' compliance. The estimated difference of Exp1P – Exp1C is 0.026 with a p-value of 0.210. This comparison indicates that individual punishment has no significant impact, when compared with the control group. In other words, with 100% detection, imposing individual punishment to noncompliant behavior does not statistically improve employees' compliance with an information security policy. Hence, Hypothesis 2 is not supported. This result suggests that the deterrence only strategy may not effectively prevent insider data breaches.

However, the estimated difference of Exp1R – Exp1C is 0.101 and highly significant with a p-value less than 0.001. This indicates that individual reward, with 100% detection, works well for regulating employees' noncompliant behavior. Therefore, Hypothesis 1 is supported. In addition, comparing Exp1RP and Exp1C, indicates a positive difference in estimated means (0.193) and an extremely small p-value (< 0.001). Furthermore, the estimated difference of Exp1RP – Exp1P is 0.167 (p-value < 0.001) and Exp1RP – Exp1R is 0.093 (p-value < 0.001). This illustrates that, with 100% detection, individual reward and punishment together is significantly better than either individual punishment or individual reward. Thus, Hypothesis 3 is strongly supported. This finding is consistent with Andreoni, Harbaugh and Vesterlund (2003) stating, "the absence of a reward is not equivalent to a punishment." Based on these results, when the ability to detect non-compliance is 100%, designing an incentive mechanism around punishment only and omitting reward is a mistake, although such a strategy is commonly used in current information security practice.

Comparing individual reward and individual punishment in complying with an information security policy, the estimated difference of Exp1R – Exp1P is positively significant with a p-value less than 0.001. This result indicates that, with 100% detection, reward is more powerful than punishment in preventing insider data breaches caused by employees. This is an interesting result, although the extant majority literature asserts that perceived punishment is more effective than perceived reward (Bulgurcu, Cavusoglu and Benbasat 2009, Bulgurcu, Cavusoglu and Benbasat 2010, Liang, Xue and Wu 2013, Pahnila, Siponen and Mahmood 2007, Siponen, Pahnila and Mahmood 2010, Vance, Siponen and Pahnila 2012). This literature all used uncompensated surveys as the measurement instruments. The uncompensated survey method suffers from self-report bias. Survey takers tend to provide socially desirable answers to questionnaires (Krumpal 2013). In addition, the survey method tends to ask participants about information security compliance in general. It is almost impossible to capture an employee's actual thought when facing temptations. Instead, the compensated approach outlined in this paper reveals the superior power of real dollar reward compared with real dollar punishment in an information security policy compliance setting.

Although violating an information security policy is a socially undesirable/unethical, even illegal behavior, a company frequently delegates the compliant responsibility to employees' ethics or moral standards (Herath and Rao 2009). Accordingly, deterrence is commonly used to enhance such effect when one's ethical or moral obligation is weak. However, employees may not actually perceive the security policy that way, especially when facing time pressure or temptations. Puhakainen (2006) argue that employees perceive that the security policy slows down their work with added procedures. The results summarized in this paper, suggest that paying a little extra reward to prevent huge data breaches is more beneficial than relying on punishment alone.

6.2. Design 2 Results and Discussion

Design 2 was conducted to study how collective sanctions (collective reward and collective punishment) influence employees' compliant behavior. Based on Table 3's statistical results, it seems that in general collective sanctions have negative impacts on employees' compliance. The estimated difference of Exp2P – Exp1C is -0.091 with a p-value less than 0.001 and the estimated difference of Exp2R – Exp1C is -0.150 with a p-value less than 0.001. This result indicates that a company is better off relying on employees' conscience or moral standards rather than using collective rewards or collective punishments. This might be the reason why it is very rare to see an American company either reward all their employees, when they are all complying, or punish all, including complaint employees, when someone is violating the security policy.

The impact of collective sanctions on employees' security compliance can be estimated by comparing individual reward with collective reward and individual punishment with collective punishment. Specifically, the estimated difference of Exp2P – Exp1P is -0.118 with a p-value less than 0.001 and the estimated difference of Exp2R – Exp1R is -0.252 with a p-value is less than 0.001. The estimated difference of Exp2RP – Exp1RP is -0.180 with a p-value is less than 0.001. All these results indicate that collective sanctions, with 100% detection, are less effective than individual sanctions (i.e., individual reward or/and individual punishment) in this research setting.

6.3. Design 3 Results and Discussion

So far, the impact of rewards and punishments on employees' security compliance has been studied in a perfect detection environment. However, as pointed out earlier, real-world detection systems are not 100% effective. Design 3 was conducted to understand how a low chance of detection influences employees' compliance behavior. The estimated difference of Exp3C – Exp1C is -0.038 with a significant p-value of 0.015. This result supports Hypothesis 4, as a low chance of detection has a negative impact on employees' compliance with a company's information security policy. Furthermore, the estimated difference of Exp3P – Exp1P is -0.117 with a p-value less than 0.001, the estimated difference of Exp3R – Exp1R is -0.069 with a p-value of 0.043, and the estimated difference of Exp3RP – Exp1RP is -0.175 with a p-value less than 0.001. These results strongly support Hypotheses 5 and 6 that a low chance of detection undermines the regulating power of individual reward or/and individual punishment.

Interestingly, individual punishment with a low probability of detection is no better than the control group with a low probability of detection, as the estimated difference of Exp3P – Exp3C is -0.050 with a p-value of 0.121. Meanwhile, individual reward and punishment, together with a low probability of detection, is also no better than individual reward only with low probability of detection: the estimated difference of Exp3RP – Exp3R is not significant with a p-value of 0.452. This finding suggests a company needs to enhance its deterrence certainty to prevent insider data breaches if the punishment mechanism is adapted, although we found that punishment only is not effective to prevent noncompliance.

6.4. Design 4 Results and Discussion

Design 4 combined a low probability of detection and collective sanctions. The estimated difference of Exp4P – Exp1C is negative (-0.123) with a p-value less than 0.001. However, the estimated difference of Exp4R – Exp1C is 0.063 with a p-value less than 0.001 and the estimated difference of Exp4RP – Exp1C is 0.057 with a p-value of 0.018. These results suggest that collective punishment with a low probability of detection is worse than the control group with 100% detection. However, collective reward with a low probability of detection outperforms the most basic control group, which relies on employees' perceived obligation for compliance. This can be a very realistic and practical incentive structure for a company to prevent its employees from violating information security policy. In order words, in an imperfect detecting environment of information security, company can reduce insider security breaches by rewarding employees monetary bonus.

Although these results are inconsistent with the findings about the general negative effect of collective sanctions in Design 2, when detection is certain; it is still interesting to learn that collective reward is superior and collective punishment is inferior even with a low probability of detection. This also demonstrates that the interactions between collective sanctions and a low probability of detection are not simple additive relationships, as both collective reward and collective punishment would be worse than the control group after controlling for the large uncertainty influence. Rather, the low chance of detection transforms the collective reward mechanism and differentiates its regulating power from collective punishment.

In addition, after controlling for the detection effect by comparing Design 4 with Design 3, we can learn how the low probability of detection changes the relationship between collective sanctions and individual sanctions. The estimated difference of Exp4P – Exp3P is negative (-.035) with a p-value of 0.012, which suggests that collective punishment is worse than individual punishment with a low probability of detection. This is consistent with a previous finding with 100% detection. On the contrary, collective reward is slightly better than individual reward with a low probability of detection: the estimated difference of Exp4R – Exp3R is 0.029 with a p-value of 0.114 (one tail is 0.057). Furthermore, the estimated mean of Exp4RP – Exp3RP is also positive (0.037) with a p-value less than 0.001. This means that collective reward and punishment together is better than individual reward and punishment together when there is a low probability of detection.

Comparing Design 4 with Design 2, the only difference between these two experiments is certainty of detection. A low probability of detection has a negative impact on collective punishment, but a positive impact on collective reward. These can be shown by the fact that estimated difference of Exp4P – Exp2P is negative (-0.032) with a p-value of 0.004, but the expected difference of Exp4R – Exp2R is positive (0.215) with a p-value less than 0.001. In addition, the estimated difference of Exp4RP – Exp2RP is 0.041 with a p-value of 0.037. This indicates that collective reward and punishment together is more effective if the probability of detection is low. When the probability of detection is low and therefore punishment is uncertain, people tend to commit more security violations. Collective sanctions mean that everyone receives punishment, including compliant people, as long as someone in the inspection list is noncompliant. Whereas, everyone receives a reward, including noncompliant ones, when everyone in the inspection list is compliant. Therefore, under collective rewards, there is no chance of compliant employees losing rewards. Considering the results in Design 4, collective rewards with a small probability of detection outperforms collective punishment with small probability of detection: the estimated difference of Exp4R – Exp4P equal to 0.188, with a p-value less than 0.001. Moreover, the expected difference of Exp4RP – Exp4R is not significant, with a p-value of 0.733; therefore, collective reward and punishment together with a small probability of detection is no better than collective reward only with a small probability of detection. This further demonstrates that reward is the preferred mechanism to regulate insider data breaches even in a collective environment with a low probability of detection.

7. Robustness, Demographic and Personal Characteristic Variables

Table 4 presents logit regression results for participants' compliance with an information security policy. The dependent variable is each participant's answer of "No" (1) or "Yes" (0) to each scenario. The independent variables include the participants' demographic and personal characteristic variables; each participant's Holt and Laury (2002) risk aversion measurement; and coded dummy variables 1 to 30 to control for the potential effects caused by the wording of 30 different scenarios.

Table 4 Logit Regression Results for Information Security Policy Compliance

Dependent Variable	Model 1	Model 2	Model 3
Exp1C	0	0	0
	(.)	(.)	(.)
Exp1P	0.0270	0.0263	0.0407
	(0.0561)	(0.0540)	(0.0574)
Exp1R	0.101^{+}	0.108*	0.117*
	(0.0572)	(0.0526)	(0.0565)
Exp1RP	0.194***	0.183***	0.202***
	(0.0536)	(0.0510)	(0.0542)
Exp2P	-0.0917	-0.0919^{+}	-0.0712
	(0.0591)	(0.0538)	(0.0578)
Exp2R	-0.152**	-0.137*	-0.140*
	(0.0540)	(0.0544)	(0.0556)
Exp2RP	0.0148	0.0133	0.0329

	(0.0615)	(0.0571)	(0.0609)
Exp3C	-0.0377	-0.0380	-0.0222
	(0.0590)	(0.0529)	(0.0571)
Exp3P	-0.0881	-0.0968^{+}	-0.0737
	(0.0553)	(0.0526)	(0.0575)
Exp3R	0.0348	0.0367	0.0475
	(0.0586)	(0.0570)	(0.0587)
Exp3RP	0.0215	0.0259	0.0377
	(0.0596)	(0.0557)	(0.0606)
Exp4P	-0.124*	-0.0941^{+}	-0.100^{+}
	(0.0561)	(0.0527)	(0.0556)
Exp4R	0.0630	0.0729	0.0878
	(0.0609)	(0.0583)	(0.0622)
Exp4RP	0.0578	0.0493	0.0698
	(0.0638)	(0.0595)	(0.0627)
Scenario Difference	Controlled	Controlled	Controlled
Risk Taking		-0.0367***	
		(0.00870)	
Impulsivity		-0.0330***	
		(0.00957)	
HL Risk Aversion		0.00206	0.00837^{+}
		(0.00481)	(0.00500)
Age		0.0227*	0.0266**
		(0.0101)	(0.00992)
Business Major		-0.00329	0.00148
		(0.0215)	(0.0221)
Non-business Major		0	0
		(.)	(.)
Computer Hours		0.00898^{+}	0.00802
		(0.00531)	(0.00550)
Gender		-	-
Dominant Hand		-	-
Computer Skills		-	-
Class		-	-
GPA		-	-
Race		-	-
Organizational Experience		-	-

Note: Marginal Effects (dy/dx) with Standard Errors in parentheses; N.A. stands for No Answer;
$^{+}$ $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$
"-" means the variable is controlled in the model but omitted for reporting due to its insignificant value

The most basic control group (i.e., Exp1C in Design 1) was the base for the categorical variables in the logit regression to test the treatment effects after controlling for the scenario differences in Model 1. Exp1RP, Exp2R, and Exp4P are significantly different from Exp1C. Exp1R is weakly significant at the 0.1 level, for compliance as well. These results are consistent with the time

series autoregressive model test for DCR: the same direction (i.e., sign) of numbers between the marginal effects of the logit regression and the expected difference of DCR (the first row of Table 3) in the time series analysis. Careful readers may wonder why the time series analysis shows more significant values than the logit regression. This is because the standard errors for the treatment effects are more precise when the unit of analysis is the treatment group. As our research question is about compliance behavior in the workplace as a group, using an individual person as the unit of analysis for studying treatment effects is not appropriate, although it can permit us to study individual differences related to compliance. Furthermore, the standard errors caused by other unobserved variables of individual difference average out when we use the treatment group as the unit of analysis, providing more accurate statistical test results for treatment effects.

The logit regression with demographic and personal traits is Model 2 of Table 4. Interestingly, the significance level and the sign of marginal effects did not change much, except the coefficient for Exp1R is now significant, the p-value increasing from 0.1 to 0.05 and Exp3P becomes marginally significant at the 0.1 level. This means that those demographic and personal traits variables should be orthogonal to the treatment variables for information security compliance. This further demonstrates the robustness of results from the time series analysis.

In addition, risk taking is negatively significant at the 0.001 level. This suggests that risk-loving employees are more likely to violate an information security policy. Furthermore, impulsivity is also negatively significant. Impulsive people were defined by Hu, West and Smarandescu (2015) as the individuals who do not take adequate time to evaluate inputs before making a decision. Hence, it makes sense that impulsive employees tend to violate information security policies more. Moreover, age is another significant factor for security compliance. The positive coefficient of age suggests that older employees are more likely to comply with an information security policy.

However, gender, dominant hand, computer skills, education level and grades, ethnicity, as well as organizational experience have no significant impact on information security compliance, although number of hours on the computer per day seems to have a weak effect. This may very well explain why insider data breaches happen so frequently no matter the workplace environment (e.g., companies, governmental sectors, universities, or other nonprofit organizations). It is worth noting that business majors are no different from non-business majors for information security compliance.

Unexpectedly, the Holt and Laury (2002)'s risk aversion's measurement is not significant in Model 2. This result may be due to multicollinearity with risk taking and impulsivity. Hence, Model 3 omits both risk taking and impulsivity. Then, risk aversion becomes weakly significant with a positive sign. The positive value suggests that risk-averse individuals are more likely to comply with an information security policy. In addition, Model 3 represents almost the same regression results as Model 2, even without two significant factors. This further shows that the demographic and personal traits are independent of the treatment variables for information security compliance. Therefore, it further demonstrates the robustness of the results from the time series data analysis.

8. Conclusions, Implications, and Limitations

Information security is important to study both as academic research as well as for industry practice. Although there has been much research into information security, including both technological defense and policy regulations, data breaches seem to become more and more common and harder to prevent. Much literature has identified that human factors, particularly employees' noncompliance with information security policies, are the fundamental causes of data breaches, as insider employees are the weakest part of security defense.

This paper aims to design a realistic incentive structure to help a company protect its information assets. This study is the first attempt to use behavioral economics techniques to explore how individual sanctions, collective sanctions, and detection mechanisms influence employees' compliance with a company's information security policy. The nature and complexity of individual reward, collective reward, individual punishment, collective punishment, a small probability of detection, and their interactions gradually unfolded through a series of sequential lab experiments. The following conclusions can be drawn from these experimental results.

First, individual reward and punishment together with 100% detection is the best strategy for a company to regulate its employees' noncompliance. The superior performance of Exp1RP compared to every other strategy demonstrates this finding. The complementary effect between reward and punishment is very strong, and thus omitting either one could be a mistake. Therefore, a company should always employ both means to achieve better regulating power, although it may cost the company to give rewards.

Second, individual reward is always better than individual punishment for security compliance. This suggests a company should rethink its managerial policy if it is deterrence based. Why do people break rules even though they know it is wrong? Don't employees understand that it is their obligation to obey the policy? It seems that employee's perception of security procedure is not in line with the company's. Hence, giving a small reward for compliant behavior aligns both parties' interests. Third, collective sanctions are a complex incentive mechanism. A company should use them with great caution. Fourth, a low probability of detection undermines the incentive power of individual rewards or/and individual punishments. Hence, a company must improve its detection systems to take full advantage of individual sanctions. This requires the joint effort of a company's technical team and managerial leadership. In addition, a low probability of detection weakens the value of punishment more than it does for reward. A company is better off either not using punishment at all or be able to detect 100% of non-compliant behavior; otherwise, punishment with a low probability of detection is worse than no punishment. Instead, if there is a low probability of detection, it is better to rely on reward. But, combining reward and punishment is superior to either reward or punishment.

Finally, a company should avoid hiring risk-loving, impulsive, and junior people (if possible) for key information security positions. To avoid discriminating against young people, a company might not hire applicants who score high on a measure of risk loving. Those employees may pose stronger threats to a company's security defense and their compliance may not be easily improved by rewards or punishments.

Reference

Abrams R (2014) Target puts data breach costs at $148 million, and forecasts profit drop. *The New York Times*.

Alaskar M, Vodanovich S, Shen KN (2015) Evolvement of information security research on employees' behavior: a systematic review and future direction. *2015 48th Hawaii International Conference on System Sciences* (IEEE), 4241-4250.

Alexander CS, Becker HJ (1978) The use of vignettes in survey research. *Public Opinion Quarterly*. 42(1):93-104.

Anderson D, Frivold T, Valdes A (1995) Next-generation intrusion detection expert system (NIDES): A summary. SRI International, http://merlot.usc.edu/cs530-s08/papers/Anderson95a.pdf.

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

Balliet D, Mulder LB, Van Lange PA (2011) Reward, punishment, and cooperation: a meta-analysis. *Psychological Bulletin*. 137(4):594-615.

Barlow JB, Warkentin M, Ormond D, Dennis AR (2013) Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*. 39(2):145-159.

Becker GS (1968) Crime and punishment: An economic approach. *The Journal of Political Economy*. 76(2):169–217.

Becker GS (1974) A theory of social interactions. *Journal of Political Economy*. 82(6):1063-1093.

Binger BR, Copple R, Hoffman E (1995) Contingent valuation methodology in the natural resource damage regulatory process: Choice theory and the embedding phenomenon. *Natural Resources Journal*. 35(1995):443-459.

Boss SR, Kirsch LJ, Angermeier I, Shingler RA, Boss RW (2009) If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*. 18(2):151-164.

Bulgurcu B, Cavusoglu H, Benbasat I (2009) Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors. *2009 International Conference on Computational Science and Engineering* (IEEE), 476-481.

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

Chang SE, Ho CB (2006) Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*. 106(3):345-361.

Chen DL, Schonger M, Wickens C (2016) oTree—An open-source platform for laboratory, online, and field experiments. *Journal of Behavioral and Experimental Finance*. 9(2016):88-97.

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

Cheng L, Li Y, Li W, Holm E, Zhai Q (2013) Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*. 39(2):447-459.

Colwill C (2009) Human factors in information security: The insider threat–Who can you trust these days? *Information Security Technical Report*. 14(4):186-196.
D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*. 20(1):79-98.
D'Arcy J, Hovav A (2009) Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*. 89(1):59-71.
Dallin DJ, Nicolaevsky BI (1947) Forced labor in Soviet Russia. Yale University Press.
Dhillon G, Backhouse J (2000) Technical opinion: Information system security management in the new millennium. *Communications of the ACM*. 43(7):125-128.
Dutta A, McCrohan K (2002) Management's role in information security in a cyber economy. *California Management Review*. 45(1):67-87.
Edney JJ, Harper CS (1978) The commons dilemma. *Environmental Management*. 2(6):491-507.
Ernst, Young (2002) Global information security survey. UK: Presentation Services.
Ernst, Young (2008) Moving beyond compliance: Ernst & Young's 2008 global information security survey. Ernst & Young, http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/2008_E&YWhitePaper_GlobalInfoSecuritySurvey.pdf.
Fehr E, Gächter S (2000) Cooperation and punishment in public goods experiments. *American Economic Review*. 90(4):980-994.
Finne T (2000) Information systems risk management: key concepts and business processes. *Computers & Security*. 19(3):234-242.
Garcia-Teodoro P, Diaz-Verdejo J, Maciá-Fernández G, Vázquez E (2009) Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*. 28(1):18-28.
Gilham SA (1982) The marines build men: resocialization in recruit training. Luhman R, eds. *Sociological Outlook: A Text With Readings* (Wadsworth Publishing Company, Belmont, CA), 231-241.
Guo KH, Yuan Y (2012) The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*. 49(6):320-326.
Guo KH, Yuan Y, Archer NP, Connelly CE (2011) Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems*. 28(2):203-236.
Harrington SJ (1996) The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*. 20(3):257-278.
Hashim MJ, Bockstedt JC (2015) Overcoming free-riding in information goods: sanctions or rewards? *2015 48th Hawaii International Conference on System Sciences* (IEEE), 4834-4843.
Heckathorn DD (1988) Collective sanctions and the creation of prisoner's dilemma norms. *American Journal of Sociology*. 94(3):535-562.
Heckathorn DD (1990) Collective sanctions and compliance norms: A formal theory of group-mediated social control. *American Sociological Review*. 55(3):366-384.
Henrich J (2006) Cooperation, punishment, and the evolution of human institutions. *Science*. 311(5769):60-61.

Herath T, Rao HR (2009) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*. 47(2):154-165.
Herath T, Rao HR (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*. 18(2):106-125.
Hoffman E, Spitzer ML (1993) Willingness to pay vs. willingness to accept: legal and economic implications. *Washington University Law Review*. 71(1):59-114.
Holt CA, Laury SK (2002) Risk aversion and incentive effects. *American Economic Review*. 92(5):1644-1655.
Hu Q, Dinev T, Hart P, Cooke D (2012) Managing employee compliance with information security policies: the critical role of top management and organizational culture. *Decision Sciences*. 43(4):615-660.
Hu Q, West R, Smarandescu L (2015) The role of self-control in information security violations: insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*. 31(4):6-48.
Hu Q, Xu Z, Dinev T, Ling H (2011) Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*. 54(6):54-60.
Ilgun K, Kemmerer RA, Porras PA (1995) State transition analysis: A rule-based intrusion detection approach. *IEEE Transactions on Software Engineering*. 21(3):181-199.
Khan L, Awad M, Thuraisingham B (2007) A new intrusion detection system using support vector machines and hierarchical clustering. *The International Journal on Very Large Data Bases*. 16(4):507-521.
Krumpal I (2013) Determinants of social desirability bias in sensitive surveys: a literature review. *Quality & Quantity*. 47(4):2025-2047.
Kumar S, Spafford EH (1995) A software architecture to support misuse intrusion detection. *Computers & Security*. 14(7):607.
Lee SM, Lee S-G, Yoo S (2004) An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*. 41(6):707-718.
Lee W, Stolfo SJ (2000) A framework for constructing features and models for intrusion detection systems. *ACM Transactions on Information and System Security (TiSSEC).* 3(4):227-261.
Liang H, Xue Y, Wu L (2013) Ensuring employees' IT compliance: Carrot or stick? *Information Systems Research*. 24(2):279-294.
Lippmann R, Haines JW, Fried DJ, Korba J, Das K (2000) The 1999 DARPA off-line intrusion detection evaluation. *Computer Networks*. 34(4):579-595.
Loch KD, Carr HH, Warkentin ME (1992) Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*. 16(2):173-186.
Lynn M, Oldenquist A (1986) Egoistic and nonegoistic motives in social dilemmas. *American Psychologist*. 41(5):529-534.
McCue A (2008) Beware the Insider Security Threat. CIO Jury, http://www.silicon.com/management/cio-insights/2008/04/17/beware-the-insider-security-threat-39188671/.
Mitnick KD, Simon WL (2002) *The art of deception: Controlling the human element of security* (John Wiley & Sons, New York, NY).

Myyry L, Siponen M, Pahnila S, Vartiainen T, Vance A (2009) What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*. 18(2):126-139.
Ostrom E, Walker J, Gardner R (1992) Covenants with and without a sword: Self-governance is possible. *American Political Science Review*. 86(2):404-417.
Padayachee K (2012) Taxonomy of compliant information security behavior. *Computers & Security*. 31(5):673-680.
Pahnila S, Siponen M, Mahmood A (2007) Employees' behavior towards IS security policy compliance. *2007 40th Annual Hawaii International Conference on System Sciences* (IEEE), 156-166.
Pogarsky G (2004) Projected offending and contemporaneous rule‐violation: Implications for heterotypic continuity. *Criminology*. 42(1):111-136.
Porras PA, Neumann PG (1997) EMERALD: Event monitoring enabling response to anomalous live disturbances. *Proceedings of the 20th National Information Systems Security Conference*, 353-365.
Puhakainen P (2006) Design theory for information security awareness. OULU University Press.
PwC (2008) Employee behaviour key to improving information security, new survey finds. https://pwc.blogs.com/press_room/2008/03/employee-behaviour-key-to-improving-information-security-new-survey-finds.html.
PwC (2015) Information security breaches survey. http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.
Rand DG, Dreber A, Ellingsen T, Fudenberg D, Nowak MA (2009) Positive interactions promote public cooperation. *Science*. 325(5945):1272-1275.
Richardson R (2008) CSI computer crime and security survey. Computer Security Institute, http://www.gocsi.com.
Rockefeller S (2014) A kill chain analysis of the 2013 target data breach. Committee on Commerce, Science and Transportation.
Sequeira K, Zaki M (2002) ADMIT: anomaly-based data mining for intrusions. *Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (ACM), 386-395.
Shogren JF, Shin SY, Hayes DJ, Kliebenstein JB (1994) Resolving differences in willingness to pay and willingness to accept. *The American Economic Review*. 84(1):255-270.
Sigmund K (2007) Punish or perish? Retaliation and collaboration among humans. *Trends in Ecology & Evolution*. 22(11):593-600.
Siponen M, Pahnila S, Mahmood MA (2010) Compliance with information security policies: An empirical investigation. *Computer*. 43(2):64-71.
Siponen M, Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*. 34(3):487-502.
Smith VL (1976) Experimental economics: Induced value theory. *The American Economic Review*. 66(2):274-279.
So MW, Sculli D (2002) The role of trust, quality, value and risk in conducting e-business. *Industrial Management & Data Systems*. 102(9):503-512.
Sommestad T, Hallberg J, Lundholm K, Bengtsson J (2014) Variables influencing information security policy compliance: a systematic review of quantitative studies. *Information Management & Computer Security*. 22(1):42-75.

Son J-Y (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*. 48(7):296-302.
Stolfo SJ, Lee W, Chan PK, Fan W, Eskin E (2001) Data mining-based intrusion detectors: an overview of the columbia IDS project. *ACM SIGMOD Record*. 30(4):5-14.
Straub Jr DW (1990) Effective IS security: An empirical study. *Information Systems Research*. 1(3):255-276.
Straub Jr DW, Nance WD (1990) Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*. 14(1):45-60.
Thomson I (2007) HMRC data loss leaves 25 million exposed. *ITN News*, http://www.itnews.com.au/news/hmrc-data-loss-leaves-25-million-exposed-97704.
Trevino LK (1992) Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly*. 2(2):121-136.
Vance A, Siponen M, Pahnila S (2012) Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*. 49(3):190-198.
Vance A, Siponen MT (2012) IS security policy violations: a rational choice perspective. *Journal of Organizational and End User Computing*. 24(1):21-41.
Vermeulen C, Von Solms R (2002) The information security management toolbox–taking the pain out of security management. *Information Management & Computer Security*. 10(3):119-125.
Von Solms B, Von Solms R (2004) The 10 deadly sins of information security management. *Computers & Security*. 23(5):371-376.
Wallace G (2014) HVAC vendor eyed as entry point for Target breach. *CNN Money*, http://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/.
Warkentin M, Willison R (2009) Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*. 18(2):101-105.
Yamagishi T (1986) The provision of a sanctioning system as a public good. *Journal of Personality and Social Psychology*. 51(1):110-116.
Yu H, Yang J, Han J (2003) Classifying large data sets using SVMs with hierarchical clusters. *Proceedings of the 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (ACM), 306-315.

Appendix A: 30 Scenarios for Information Security Policy Violations*

Scenario # [unknown to participants]	Severity (personal benefits) [unknown to participants]	Scenario Content and Decision-making Question [known to participant]
Scenario 1	Minor (1 tokens)	Josh's mentor Mary is worried about her job security and wanted to know if her position is among those that are being considered for elimination.
		Should Josh access the secure server and find the data? No? Yes?
Scenario 2	Minor (2 tokens)	Josh received an e-mail from his college professor who asked Josh to talk about the details of IT security management, which is considered confidential, in a seminar.
		Should Josh honor his professor's request? No? Yes?
Scenario 3	Major (27 tokens)	Josh's boss Christine wanted to know the compensation information of the top executives in the company. Josh could earn substantial favors from Christine.
		Should Josh access the secure server and get the data for Christine? No? Yes?
Scenario 4	Major (19 tokens)	Josh's company is about to release quarterly earnings. If he can act early before the information is public, he could make a substantial profit on the stock market.
		Should Josh find out the earnings data and act accordingly? No? Yes?
Scenario 5	Major (26 tokens)	Jeff is an IT consultant Josh met at a seminar. Jeff wants a copy of the detailed computer network map of the company, and offers Josh a chance of making a substantial amount of money on a consulting project.
		Should Josh provide the map? No? Yes?
Scenario 6	Major (22 tokens)	Josh's buddy Mike, who works in the sales department, wanted to know the prices of competitors for similar products to those he is selling, and promised to share commission.
		Should Josh access competitors' computers and find the data? No? Yes?
Scenario 7	Minor (1 tokens)	Josh's brother-in-law Kevin, who is a salesperson for a local firm, wanted to know if a particular type of material is used in the new product under development.
		Should Josh access the secure server and find the data? No? Yes?

Scenario 8	Major (21 tokens)	At a dinner with friends, Josh was introduced to a stranger who asked if Josh knows the bidding price of a component from suppliers, and promised to share commission.
		Should Josh get the price for this stranger? No? Yes?
Scenario 9	Major (26 tokens)	Josh's girlfriend Jenny, who works for a consulting firm, wanted to have some information about suppliers. Jenny could earn a substantial amount of commission.
		Should Josh access the secure server and find the data for Jenny? No? Yes?
Scenario 10	Minor (4 tokens)	Josh has invested a significant portion of his money in his company stock. The new product under development is going to have a significant impact on the stock price.
		Should Josh find internal documents about the new product? No? Yes?
Scenario 11	Major (30 tokens)	Josh's mentor Mary was laid off due to downsizing. Josh is very upset about this and considering doing something to take revenge.
		Should Josh delete crucial computer files to vent his anger? No? Yes?
Scenario 12	Major (17 tokens)	Josh's friend Mike, who works for an investment firm, wanted to know the quarterly earnings data before public release, and promised to share any profit from this data.
		Should Josh access the secure server and get the data for Mike? No? Yes?
Scenario 13	Major (27 tokens)	Josh has been upset about not receiving an anticipated salary increase in the last annual evaluation. He knows some underground websites offering to pay for credit card data.
		Should Josh sell customer credit card information? No? Yes?
Scenario 14	Minor (8 tokens)	Josh's buddy Mike, who works for an investment firm, wanted to know how close a new product under development is in commercial production.
		Should Josh access the secure server and find the data? No? Yes?
Scenario 15	Minor (1 tokens)	Josh met Frank at an industry conference in Las Vegas. Frank asks Josh if he could give him the IP address of a highly protected computer server for testing.
		Should Josh find out the IP address for Frank? No? Yes?
Scenario 16	Major (26 tokens)	Josh belongs to a citizens' group that advocates hiring local workers. The group wants Josh to provide some confidential evidence to support a lawsuit. Josh would share any settlement money if the group wins.
		Should Josh provide the confidential data to the group?

		No? Yes?
Scenario 17	Major (23 tokens)	Josh's brother-in-law Kevin, who is a salesperson for a local firm, wanted to get contract information of suppliers, and promised to share a substantial amount of commission.
		Should Josh get the information for Kevin? No? Yes?
Scenario 18	Minor (8 tokens)	Josh's girlfriend Jenny, who works for a consulting firm, wanted to know whether one of her clients is involved in the new product development with his firm.
		Should Josh access the secure server and find the data? No? Yes?
Scenario 19	Major (15 tokens)	Josh met Frank at an industry conference in Las Vegas. Frank asks Josh if he could give him the IP address of a highly protected computer server for testing, and promises to help Josh find consulting work.
		Should Josh give Frank the information? No? Yes?
Scenario 20	Major (20 tokens)	Josh must complete a project by this Friday and one way to speed up the progress is to copy source code from other companies that he knows have done similar projects.
		Should Josh hack into a competitor's computer and copy the code? No? Yes?
Scenario 21	Minor (5 tokens)	Josh's best friend Eric, who works for a competitor, wanted to know whether a new product under development has certain features.
		Should Josh access the secure server and find the data? No? Yes?
Scenario 22	Major (27 tokens)	Josh's friend Julie, who is an HR manager, asks Josh to find the payroll information of peer companies for her benchmark study, and promises Josh to help in the future.
		Should Josh access the payroll data on peer companies' servers? No? Yes?
Scenario 23	Minor (2 tokens)	Josh belongs to a citizens' group that advocates hiring local workers. The group wanted to confirm whether Josh's company is outsourcing jobs to offshore suppliers.
		Should Josh access the secure server and find it out? No? Yes?
Scenario 24	Minor (8 tokens)	The only way for Josh to meet the deadline this Friday is to bring some files home to work on his computer in the evenings, which is explicitly prohibited by the company.
		Should Josh bring the files home and work on his computer? No? Yes?

Scenario 25	Minor (5 tokens)	Josh is not sure how much he should be asking for a salary raise or even if he should be asking at all given the financial situation of the company.
		Should Josh access the secure server and find more information? No? Yes?
Scenario 26	Minor (4 tokens)	Josh's friend, Jane, works in the HR department as a payroll specialist. Jane asked Josh to change the payroll data file to erase the unpaid vacation hours she had taken.
		Should Josh make the changes on the server for Jane? No? Yes?
Scenario 27	Major (16 tokens)	Josh's buddy Eric, who works for a competitor, wanted to get a critical design in the new product under development, and promises to pay a substantial amount of money.
		Should Josh access the secure server and find the data for Eric? No? Yes?
Scenario 28	Minor (3 tokens)	Josh's boss Christine wanted to know about the executive compensation information of the company, which is confidential.
		Should Josh access the secure server and find the data? No? Yes?
Scenario 29	Minor (4 tokens)	At a dinner with friends Josh was introduced to a stranger who asked if Josh knows the price of a component for which Josh's company is requesting bids from suppliers.
		Should Josh get the price on a secure server for this stranger? No? Yes?
Scenario 30	Minor (2 tokens)	Josh's buddy Mike, who works in the sales department of the same company, wanted to know if another account manager in the company is about to close a major deal.
		Should Josh access the secure server and get the information? No? Yes?

*All 30 scenarios were adapted from Hu, West and Smarandescu (2015).

Appendix B: Experiment Instructions

General Introduction

Thank you for participating in this study, and please read the following instructions carefully. If you have any questions, do not hesitate to ask us. Aside from this, no communication is allowed during the experiment.

This study is about information security and decision making. You MUST be least 18 years old to participate. This lab session is completely anonymous and will take approximately 45 minutes to complete. You will earn $10 on average and your final compensation may vary depending on your decisions made on the study tasks. Everything will be paid to you in cash/check immediately after the experiment.

Now, you are given 500 endowment tokens to participate in this study and **imagine that you are an employee, named Josh:** [Core Instruction]

> *Josh works for the IT department of a large global manufacturing company that supplies sophisticated electronic control instruments for civilian and military uses. Over the years Josh has developed knowledge and skills that enable him to access almost any computer and database in his company with or without authorization.*
>
> *[Exp1C] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data.*
>
> *Josh has been working on multiple projects recently, some with deadlines in one or two weeks. Josh is under tremendous pressure to meet the deadlines of his boss. Josh is also financially stressed and he is behind in some payments for his bills and credit cards. For each of the given circumstances, Josh will gain some benefits from 0 to 30 tokens if he chooses to do things that are favorable to him or his friends. The more severe of the scenarios, the more profits Josh would obtain.*
>
> For your convenience, these instructions will remain available to you on all subsequent screens of this study.

Again, imagine that you are Josh and complete a number of scenario-based tasks on behalf of Josh on the following screens. **Josh's final income of tokens from the**

experiment will be converted to dollars and given to you at the end of the study. The exchange rate is 100 tokens = $1.3.

Now, please write down the three-digit random number which is given to you in the beginning of the study to start the lab: _____

Interventions for Design 1-4

All other is the same as illustrated above except for the paragraph labeled as "*[Exp1C]*". The rest treatments of our four designs are listed as the followings:

[Exp1R] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately established a new policy to give 10 tokens to those employees who are protecting the company's information assets for each circumstance.

[Exp1P] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately established a new policy to deduct 10 tokens from those employees who are not protecting the company's information assets for each circumstance.

[Exp1RP] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately established a new policy to give 10 tokens to those employees who are protecting the company's information assets, but deduct 10 tokens from those employees who are not protecting the company's information assets for each circumstance.

[Exp2R] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately established a new policy to give 10 tokens to ***all employees*** *only when all employees are protecting the company's information assets for each circumstance.*

[Exp2P] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately established a new policy to deduct 10 tokens from ***all employees*** *as long as someone is not protecting the company's information assets for each circumstance.*

[Exp2RP] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately established a new policy to give 10 tokens to ***all employees*** *only when all*

employees are protecting the company's information assets, but deduct 10 tokens from ***all employees*** *as long as someone is not protecting the company's information assets for each circumstance.*

[Exp3C] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately installed a detecting system which will inspect 20% of its employees to check if they are protecting its information assets.

[Exp3R] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately installed a detecting system which will inspect 20% of its employees to check if they are protecting its information assets. In addition, the company also established a new policy to give 10 tokens to those selected employees who are protecting the company's information assets for each circumstance.

[Exp3P] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately installed a detecting system which will inspect 20% of its employees to check if they are protecting its information assets. In addition, the company also established a new policy to deduct 10 tokens from those selected employees who are not protecting the company's information assets for each circumstance.

[Exp3RP] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately installed a detecting system which will inspect 20% of its employees to check if they are protecting its information assets. In addition, the company also established a new policy to give 10 tokens to those selected employees who are protecting the company's information assets, but deduct 10 tokens from those selected employees who are not protecting the company's information assets for each circumstance.

[Exp4R] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately installed a detecting system which will inspect 20% of its employees to check if they are protecting its information assets. In addition, the company also established a new policy to give 10 tokens to ***all employees*** *only when all selected employees are protecting the company's information assets for each circumstance.*

[Exp4P] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately installed a detecting system which will inspect 20% of its employees to check if they are protecting its information assets. In addition, the company also established a new policy to deduct 10 tokens from ***all employees*** *as long as someone among the selected employees is not protecting the company's information assets for each circumstance.*

[Exp4RP] The company has explicit and strict policies against any unauthorized access, copy, transfer, or use of its digital assets, including confidential or non-confidential data. The company lately installed a detecting system which will inspect 20% of its employees to check if they are protecting its information assets. In addition, the company also established a new policy to give 10 tokens to ***all employees*** *only when all selected employees are protecting the company's information assets, but deduct 10 tokens from* ***all employees*** *as long as someone among the selected employees is not protecting the company's information assets for each circumstance.*

Appendix C: Detailed Experimental Design

Design 1

In this experiment, we simply examine how reward and punishment influence participants' decision making. A 2 x 2 factorial design is presented here,

Control group. oTree presents subjects with all 30 scenarios. For each scenario, oTree records their choices. In addition, participants are informed that they have a chance to earn an additional 0 to 30 tokens if they choose "Yes".

Reward only group. oTree presents subjects with all 30 scenarios. For each scenario, oTree adds 10 tokens if the subject chooses "No". No tokens are given to those subjects who choose "Yes". Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes".

Punishment only group. oTree presents subjects with all 30 scenarios. For each scenario, oTree deducts 10 tokens if the subject chooses "Yes". No tokens are given to those subjects who choose "No". Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes".

Reward & Punishment group. oTree presents subjects with all 30 scenarios. For each scenario, oTree adds 10 tokens if the subject chooses "No" and deducts 10 tokens if the subject chooses "Yes". Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes".

Design 2

In this experiment, we introduce the Collective Sanctions (rewarding all or punishing all) to compare the results with Experiment 1's. Since the Collective Sanctions only exist when main treatments (Reward or Punishment) are given, there is no control group in this experiment.

Collective Reward only group. oTree presents subjects with all 30 scenarios. For each scenario, oTree adds 10 tokens to every subject only when no subjects choose "Yes". No tokens are given to subjects under any other circumstances. Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes".

Collective Punishment only group. oTree presents subjects with all 30 scenarios. For each scenario, oTree deducts 10 tokens from every subject as long as there are subjects choosing "Yes". No tokens will be given to subjects under any other circumstances. Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes".

Collective Reward & Punishment group. oTree presents subjects with all 30 scenarios. For each scenario, oTree adds 10 tokens to every subject only when no subjects choose "Yes." oTree deducts 10 tokens from every subject as long as there are subjects choosing "Yes". Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes".

Design 3

In this experiment, we examine how reward and punishment influence participants' decision making when there is uncertainty that only 20% of them will be inspected. Another 2 x 2 factorial design is presented here,

Control with Inspection group. For each scenario, after all subjects have made their decisions, the oTree software randomly selects 20% of the participants to examine their choices. Those examined participants are informed that their decisions are captured by the "company", but no tokens are taken from or given to those selected participants. Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes" whether they are selected or not.

Reward only with Inspection group. For each scenario, after all subjects have made their decisions, the oTree software randomly selects 20% of the participants to examine their choices. oTree adds 10 tokens to the selected ones if they choose "No". No tokens are given to those selected subjects who choose "Yes". Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes" whether they are selected or not.

Punishment only with Inspection group. For each scenario, after all subjects have made their decisions, the oTree software randomly selects 20% of the participants to examine their choices. oTree deducts 10 tokens from the selected ones if they choose "Yes". No tokens are given to those selected subjects who choose "No". Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes" whether they are selected or not.

Reward & Punishment with Inspection group. For each scenario, after all subjects have made their decisions, the oTree software randomly selects 20% of the participants to examine their choices. oTree adds 10 tokens to the selected ones if they choose "No" and deducts 10 tokens from the selected ones if they choose "Yes". Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes" whether they are selected or not.

Design 4

In this experiment, we introduce the Collective Sanctions (rewarding all or punishing all) again based on Experiment 3. Since the Collective Sanctions only exist when main treatments (Reward or Punishment) are given, there is no control group in this experiment, either.

Collective Reward only with Inspection group. For each scenario, after all subjects have made their decisions, the oTree software randomly selects 20% of the participants to examine their choices. oTree adds 10 tokens to everyone, including non-selected subjects, if no selected subjects choose "Yes". No tokens are given to subjects under any other circumstances. Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes" whether they are selected or not.

Collective Punishment only with Inspection group. For each scenario, after all subjects have made their decisions, the oTree software randomly selects 20% of the participants to examine their choices. oTree deducts 10 tokens from everyone, including non-selected subjects, if one or more selected subjects choose "Yes". No tokens are given to subjects under any other circumstances. Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes" whether they are selected or not.

Collective Reward & Punishment with Inspection group. For each scenario, after all subjects have made their decisions, the oTree software randomly selects 20% of the participants to examine their choices. oTree adds 10 tokens to everyone, including non-selected subjects, if no selected subjects choose "Yes" or oTree deducts 10 tokens from everyone, including non-selected subjects, if one or more selected subjects choose "Yes". Additionally, the chance to gain 0 to 30 tokens as aforementioned is still applicable to those subjects who choose "Yes" whether they are selected or not.

Appendix D: Brief Questionnaire for Demographic and Personal Characteristic Variables

Section I: (please check one)

Age	o _____ o No Answer	**Class**	o Freshman o Sophomore o Junior o Senior o No Answer
Gender	o Male o Female o Other_____ o No Answer	**GPA**	o 2.0 – 2.5 o 2.6 – 2.9 o 3.0 – 3.5 o 3.6 – 4.0 o No Answer
Dominant hand	o Right o Left o No Answer	**Primary ethnicity/race**	o White o Hispanic or Latino o Black or African American o Asian/Pacific Islander o Other _____ o No Answer
Major	o Accounting o Finance o Marketing o Management o MIS o SCM o Other _____	**Organizational Experience**	o Full-time employee o Part-time employee o Student Internship o Never worked
Computer Skills	o Personal use only o Microsoft Office skills o Programming o Hardware and software o Advanced knowledge	**Average hours of using computers per day**	o < 3 (Specify: _____) o 3 o 4 o 5 o > 6 (Specify: _____)

Section II[**]**:** (please circle the numbers)

1-Strongly Disagree	**4-Neutral**						**7-Strongly Agree**
IP1	I often act on the spur of the moment without stopping to think.	1	2	3	4	5	6	7
IP2	I don't devote much thought and effort to preparing for the future.	1	2	3	4	5	6	7
IP3	I often do whatever brings me pleasure here and now, even at the cost of some distant goal.	1	2	3	4	5	6	7
IP4	I'm more concerned with what happens to me in the short run than in the long run.	1	2	3	4	5	6	7
RS1	I like to test myself every now and then by doing something a little risky.	1	2	3	4	5	6	7
RS2	Sometimes I will take a risk just for the fun of it.	1	2	3	4	5	6	7
RS3	I sometimes find it exciting to do things for which I might get in trouble.	1	2	3	4	5	6	7
RS4	Excitement and adventure are more important to me than security.	1	2	3	4	5	6	7
Key: IP—Impulsivity and RS—Risk taking								

(** the order of the questions in this **section II** was randomly presented to subjects)

Above survey questions were also adapted from Hu, West and Smarandescu (2015).

Section III: (please mark the boxes)

For each of the ten paired lottery choices in the following table, please check the box next to your preferred option, either Option A or Option B. Imagine throwing a ten-sided die. Each outcome (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) is equally likely. For instance, if you choose Option A in the Row No. 1 shown below, you will have a 1 in 10 chance of earning $2.00 and a 9 in 10 chance of earning $1.60. Similarly, Option B of Row No. 1 offers a 1 in 10 chance of earning $3.85 and a 9 in 10 chance of earning $0.10. Please keep in mind that as you move down the table, the chances of the higher payoff for each Option A or B increases.

Row Number	Option A		Option B	
1	$2.00 if the die's number is 1 $1.60 if the die's number is 2-10	☐	$3.85 if the die's number is 1 $0.10 if the die's number is 2-10	☐
2	$2.00 if the die's number is 1-2 $1.60 if the die's number is 3-10	☐	$3.85 if the die's number is 1-2 $0.10 if the die's number is 3-10	☐
3	$2.00 if the die's number is 1-3 $1.60 if the die's number is 4-10	☐	$3.85 if the die's number is 1-3 $0.10 if the die's number is 4-10	☐
4	$2.00 if the die's number is 1-4 $1.60 if the die's number is 5-10	☐	$3.85 if the die's number is 1-4 $0.10 if the die's number is 5-10	☐
5	$2.00 if the die's number is 1-5 $1.60 if the die's number is 6-10	☐	$3.85 if the die's number is 1-5 $0.10 if the die's number is 6-10	☐
6	$2.00 if the die's number is 1-6 $1.60 if the die's number is 7-10	☐	$3.85 if the die's number is 1-6 $0.10 if the die's number is 7-10	☐
7	$2.00 if the die's number is 1-7 $1.60 if the die's number is 8-10	☐	$3.85 if the die's number is 1-7 $0.10 if the die's number is 8-10	☐
8	$2.00 if the die's number is 1-8 $1.60 if the die's number is 9-10	☐	$3.85 if the die's number is 1-8 $0.10 if the die's number is 9-10	☐
9	$2.00 if the die's number is 1-9 $1.60 if the die's number is 10	☐	$3.85 if the die's number is 1-9 $0.10 if the die's number is 10	☐
10	$2.00 if the die's number is 1-10	☐	$3.85 if the die's number is 1-10	☐

Above Risk Aversion measurement was adapted from Holt and Laury (2002).

Appendix E: Time Series Autoregressive Model (AR=1) Data-analysis Result

91-DCR	*ar1.coef*	*ar1.p-value*	*ar1.se*	*ar1.t-ratio*	*const.coef*	*const.p-value*	*const.se*	*const.t-ratio*
Exp1P-Exp1C	-0.0940	0.6461	0.2046	-0.4592	0.0261	0.2097	0.0208	1.2544
Exp1R-Exp1C	0.0934	0.6238	0.1904	0.4905	0.1014	0.0000	0.0227	4.4614
Exp1RP-Exp1C	-0.0390	0.8389	0.1920	-0.2033	0.1934	0.0000	0.0169	11.4298
Exp2P-Exp1C	0.0224	0.9063	0.1898	0.1178	-0.0915	0.0000	0.0184	-4.9665
Exp2R-Exp1C	0.1660	0.3822	0.1899	0.8739	-0.1502	0.0000	0.0258	-5.8109
Exp2RP-Exp1C	0.2137	0.2468	0.1845	1.1581	0.0158	0.4653	0.0217	0.7301
Exp3C-Exp1C	0.1019	0.5899	0.1890	0.5390	-0.0376	0.0153	0.0155	-2.4258
Exp3P-Exp1C	0.2402	0.1802	0.1792	1.3401	-0.0874	0.0028	0.0293	-2.9839
Exp3R-Exp1C	0.3486	0.0388	0.1687	2.0663	0.0353	0.2129	0.0284	1.2456
Exp3RP-Exp1C	0.3347	0.0469	0.1685	1.9868	0.0220	0.3688	0.0245	0.8987
Exp4P-Exp1C	0.0943	0.6117	0.1858	0.5077	-0.1229	0.0000	0.0242	-5.0728
Exp4R-Exp1C	0.0751	0.6779	0.1808	0.4154	0.0632	0.0003	0.0176	3.5829
Exp4RP-Exp1C	0.2441	0.1621	0.1746	1.3982	0.0574	0.0184	0.0244	2.3568
Exp1R-Exp1P	-0.3320	0.0606	0.1769	-1.8765	0.0745	0.0000	0.0096	7.7173
Exp1RP-Exp1P	-0.0937	0.6174	0.1876	-0.4995	0.1671	0.0000	0.0146	11.4299
Exp2P-Exp1P	-0.1017	0.6176	0.2037	-0.4993	-0.1185	0.0000	0.0178	-6.6590
Exp2R-Exp1P	0.0771	0.7134	0.2099	0.3673	-0.1789	0.0000	0.0288	-6.2226
Exp2RP-Exp1P	0.2153	0.3300	0.2210	0.9741	-0.0137	0.6350	0.0289	-0.4746
Exp3C-Exp1P	-0.2580	0.1763	0.1908	-1.3524	-0.0630	0.0000	0.0137	-4.5965
Exp3P-Exp1P	0.2448	0.2557	0.2153	1.1366	-0.1174	0.0003	0.0327	-3.5918
Exp3R-Exp1P	0.2373	0.2366	0.2005	1.1836	0.0052	0.8768	0.0336	0.1550
Exp3RP-Exp1P	0.1975	0.3432	0.2084	0.9478	-0.0075	0.7766	0.0265	-0.2838
Exp4P-Exp1P	-0.1816	0.3887	0.2107	-0.8619	-0.1503	0.0000	0.0168	-8.9335
Exp4R-Exp1P	0.0270	0.8945	0.2039	0.1326	0.0358	0.1314	0.0238	1.5085
Exp4RP-Exp1P	0.1842	0.3630	0.2025	0.9097	0.0284	0.2677	0.0256	1.1083
Exp1RP-Exp1R	-0.0430	0.8115	0.1805	-0.2385	0.0930	0.0000	0.0125	7.4217
Exp2P-Exp1R	0.1445	0.4410	0.1875	0.7705	-0.1922	0.0000	0.0214	-8.9951
Exp2R-Exp1R	0.1381	0.4817	0.1962	0.7036	-0.2523	0.0000	0.0284	-8.8950
Exp2RP-Exp1R	0.3026	0.1197	0.1944	1.5561	-0.0872	0.0031	0.0294	-2.9624
Exp3C-Exp1R	-0.0094	0.9596	0.1859	-0.0506	-0.1384	0.0000	0.0156	-8.8790
Exp3P-Exp1R	0.2814	0.1552	0.1979	1.4215	-0.1905	0.0000	0.0298	-6.3989
Exp3R-Exp1R	0.3379	0.0631	0.1818	1.8588	-0.0688	0.0434	0.0341	-2.0194
Exp3RP-Exp1R	0.4233	0.0175	0.1781	2.3771	-0.0833	0.0043	0.0291	-2.8578
Exp4P-Exp1R	0.0113	0.9542	0.1969	0.0575	-0.2244	0.0000	0.0181	-12.3837
Exp4R-Exp1R	0.2469	0.1841	0.1859	1.3284	-0.0391	0.1213	0.0252	-1.5492
Exp4RP-Exp1R	0.2913	0.1134	0.1840	1.5830	-0.0462	0.0656	0.0251	-1.8408
Exp2P-Exp1RP	0.1397	0.4605	0.1893	0.7379	-0.2848	0.0000	0.0210	-13.5599
Exp2R-Exp1RP	0.1305	0.5015	0.1941	0.6722	-0.3450	0.0000	0.0305	-11.3192
Exp2RP-Exp1RP	0.5656	0.0012	0.1740	3.2495	-0.1802	0.0000	0.0379	-4.7615
Exp3C-Exp1RP	-0.2805	0.1080	0.1745	-1.6070	-0.2306	0.0000	0.0114	-20.2704
Exp3P-Exp1RP	0.3527	0.0609	0.1882	1.8740	-0.2831	0.0000	0.0341	-8.3019
Exp3R-Exp1RP	0.4387	0.0106	0.1717	2.5554	-0.1618	0.0000	0.0378	-4.2748

Exp3RP-Exp1RP	0.3923	0.0268	0.1771	2.2148	-0.1745	0.0000	0.0283	-6.1705
Exp4P-Exp1RP	0.1197	0.5327	0.1919	0.6239	-0.3169	0.0000	0.0231	-13.7227
Exp4R-Exp1RP	0.0405	0.8325	0.1917	0.2115	-0.1307	0.0000	0.0192	-6.8161
Exp4RP-Exp1RP	0.3648	0.0380	0.1759	2.0744	-0.1393	0.0000	0.0252	-5.5341
Exp2R-Exp2P	0.0995	0.5945	0.1869	0.5323	-0.0601	0.0004	0.0170	-3.5461
Exp2RP-Exp2P	0.0219	0.9085	0.1906	0.1150	0.1064	0.0000	0.0155	6.8798
Exp3C-Exp2P	0.0632	0.7593	0.2064	0.3064	0.0535	0.0005	0.0154	3.4774
Exp3P-Exp2P	0.1735	0.3598	0.1895	0.9158	0.0024	0.9044	0.0200	0.1202
Exp3R-Exp2P	0.2483	0.1820	0.1860	1.3347	0.1242	0.0000	0.0197	6.3006
Exp3RP-Exp2P	0.1086	0.5717	0.1920	0.5655	0.1123	0.0000	0.0152	7.3895
Exp4P-Exp2P	-0.0843	0.6400	0.1803	-0.4677	-0.0320	0.0035	0.0110	-2.9166
Exp4R-Exp2P	-0.3260	0.0625	0.1750	-1.8628	0.1560	0.0000	0.0107	14.5218
Exp4RP-Exp2P	0.0365	0.8578	0.2035	0.1792	0.1491	0.0000	0.0161	9.2911
Exp2RP-Exp2R	-0.3481	0.0405	0.1699	-2.0490	0.1678	0.0000	0.0130	12.8766
Exp3C-Exp2R	0.3907	0.0495	0.1989	1.9642	0.1099	0.0003	0.0307	3.5788
Exp3P-Exp2R	-0.0117	0.9500	0.1869	-0.0626	0.0638	0.0000	0.0147	4.3342
Exp3R-Exp2R	-0.0565	0.7657	0.1896	-0.2980	0.1871	0.0000	0.0170	10.9957
Exp3RP-Exp2R	-0.0624	0.7464	0.1928	-0.3234	0.1738	0.0000	0.0168	10.3283
Exp4P-Exp2R	-0.0371	0.8394	0.1832	-0.2026	0.0282	0.0596	0.0150	1.8837
Exp4R-Exp2R	-0.1273	0.4925	0.1855	-0.6864	0.2154	0.0000	0.0179	12.0212
Exp4RP-Exp2R	-0.1114	0.5783	0.2004	-0.5558	0.2106	0.0000	0.0197	10.6663
Exp3C-Exp2RP	0.2993	0.1337	0.1995	1.4997	-0.0536	0.0343	0.0253	-2.1168
Exp3P-Exp2RP	-0.1820	0.3025	0.1766	-1.0310	-0.1028	0.0000	0.0153	-6.7187
Exp3R-Exp2RP	0.1248	0.4924	0.1819	0.6864	0.0196	0.2198	0.0160	1.2272
Exp3RP-Exp2RP	0.0976	0.5989	0.1855	0.5259	0.0064	0.7024	0.0167	0.3821
Exp4P-Exp2RP	-0.1573	0.3871	0.1819	-0.8649	-0.1391	0.0000	0.0148	-9.3904
Exp4R-Exp2RP	0.1071	0.5594	0.1835	0.5837	0.0480	0.0063	0.0176	2.7311
Exp4RP-Exp2RP	0.2277	0.2550	0.2000	1.1382	0.0415	0.0372	0.0199	2.0841
Exp3P-Exp3C	0.3831	0.0408	0.1873	2.0459	-0.0497	0.1206	0.0320	-1.5523
Exp3R-Exp3C	0.4513	0.0080	0.1702	2.6510	0.0723	0.0307	0.0334	2.1612
Exp3RP-Exp3C	0.4556	0.0089	0.1742	2.6156	0.0591	0.0107	0.0232	2.5507
Exp4P-Exp3C	0.1687	0.4068	0.2034	0.8295	-0.0846	0.0000	0.0197	-4.2925
Exp4R-Exp3C	-0.0780	0.6808	0.1896	-0.4114	0.1006	0.0000	0.0162	6.1939
Exp4RP-Exp3C	0.2060	0.2509	0.1794	1.1482	0.0949	0.0000	0.0187	5.0871
Exp3R-Exp3P	-0.1559	0.3878	0.1805	-0.8636	0.1232	0.0000	0.0127	9.6684
Exp3RP-Exp3P	-0.1538	0.4024	0.1837	-0.8373	0.1098	0.0000	0.0140	7.8167
Exp4P-Exp3P	0.0416	0.8294	0.1928	0.2155	-0.0353	0.0118	0.0140	-2.5166
Exp4R-Exp3P	-0.1309	0.4727	0.1822	-0.7181	0.1511	0.0000	0.0169	8.9620
Exp4RP-Exp3P	-0.1726	0.3754	0.1947	-0.8865	0.1465	0.0000	0.0157	9.3457
Exp3RP-Exp3R	0.1468	0.4104	0.1783	0.8233	-0.0133	0.4516	0.0177	-0.7527
Exp4P-Exp3R	0.0651	0.7287	0.1876	0.3468	-0.1580	0.0000	0.0179	-8.8461
Exp4R-Exp3R	0.1863	0.2945	0.1777	1.0482	0.0286	0.1144	0.0181	1.5786
Exp4RP-Exp3R	0.1736	0.3486	0.1852	0.9374	0.0225	0.2492	0.0195	1.1522
Exp4P-Exp3RP	-0.0864	0.6500	0.1904	-0.4537	-0.1457	0.0000	0.0134	-10.9140
Exp4R-Exp3RP	0.0069	0.9697	0.1804	0.0380	0.0415	0.0017	0.0132	3.1321

Exp4RP-Exp3RP	-0.1822	0.3221	0.1840	-0.9901	0.0367	0.0005	0.0105	3.4925
Exp4R-Exp4P	-0.3100	0.0742	0.1737	-1.7853	0.1879	0.0000	0.0135	13.8946
Exp4RP-Exp4P	-0.1850	0.3541	0.1997	-0.9266	0.1829	0.0000	0.0140	13.0703
Exp4RP-Exp4R	-0.0566	0.7617	0.1866	-0.3033	-0.0050	0.7335	0.0146	-0.3405