2017

Information security research: External hacking, insider breach, and profound technologies

Yuanxiang Li
Iowa State University

Information security research: External hacking, insider breach, and profound technologies

by

Yuanxiang John Li
(Yuanxiang Li)

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Business and Technology (Information Systems)

Program of Study Committee:
Elizabeth Hoffman, Co-major Professor
Dan Zhu, Co-major Professor
James A. Davis
Zhengrui Jiang
Huaiqing Wu
Sunanda Roy

Iowa State University

Ames, Iowa

2017

DEDICATION

This dissertation is dedicated to my families, especially my wife, Yang Cui, for their continuous support. They are my ultimate motivation to pursue my doctoral degree and finish this dissertation.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I would like to thank my committee chairs, Dr. Elizabeth Hoffman and Dr. Dan Zhu, as well as my committee members, Dr. James A. Davis, Dr. Zhengrui Jiang, Dr. Huaiqing Wu, and Dr. Sunanda Roy, for their guidance and support throughout the course of this research.

In addition, I would also like to thank my friends, colleagues, the department faculty and staff for making my time at Iowa State University a wonderful experience. Particularly, I would like to express my sincere gratitude to Dr. Kenneth J. Koehler, Dr. William Q. Meeker, Dr. Helle Bunzel, Dr. Haiyang Feng, Dr. Linlin Chai, Dr. Inmyung Choi, and Yang He, for their generous help of improving this dissertation. I also want to offer my appreciation to those who were willing to participate in my studies, without whom, this dissertation would not have been possible.

ABSTRACT

Information assets are one of the most valuable intangible productive capital for a company to compete with its rivals, to learn consumers' shopping habits, to guide its development directions, and to standout to retain its profitability. However, with the Internet's characteristic of pervasiveness, information breaches from both external hacking and internal corruption are continuously encroaching a company's economic profit. This dissertation consists of three studies where each study investigates the different aspects of information security, and it is aimed to address the growing concern of securing a company's information assets. The first study examines the external hackers' behaviors and models a Bayesian game between a firm and two discrete types of hackers (domestic and international) based on the framework of Inspection Game. This study explains why external hackings, especially the international ones, are hard to prevent effectively. The second study is an empirical work and explores the other side of information security data breach, which is mainly due to insiders' (e.g., employee) malicious deeds or noncompliance with information security policy. This study shows that individual reward and punishment together with 100% detection is the best incentive structure to reduce insider data breaches. In addition, the second study finds that individual reward is more effective than individual punishment, which can better explain why employees are more willing to spend time to comply with security policy when a reward is present. Lastly, the third study is a conceptual work and relies on the Theory of Bounded Rationality to discuss how the Blockchain technology can undermine the motivations of both external and internal intruders in order to prevent information breaches. Overall, this dissertation discusses the current issues of hacking, constructs a payment/incentive structure to regulate noncompliance, empirically tests the validity

of the proposed structure, points out a solution to advance information security defense, and provides some managerial recommendations to practitioners.

CHAPTER 1. INTRODUCTION

With the rapid development of Information Technology, comes numerous opportunities for corporations to grow, but also exposes those corporations to an increasing number of potential risks caused by data breaches. According to *The New York Times* report on October 7th 2016, the U.S. government formally accused the Russian government of stealing and disclosing emails from the Democratic National Committee and a range of other institutions and prominent individuals in order to interfere with the U.S. presidential election process (Sanger and Savage 2016). If hackers could manipulate the country's presidential election, what else can they do? It constitutes a huge threat to the national security system. Meanwhile, a large number of organizations' databases are constantly comprised by external and internal intruders. Hence, this three-essay dissertation examines the information security issues from both outside hacking and inside employee non-compliance including intentional and unintentional. Moreover, the third essay of this dissertation focuses on the application of a disruptive technology, Blockchain, in advancing information security defense. As a whole, this dissertation discusses the current issues of hacking, constructs a payment/incentive structure to regulate noncompliance, empirically tests the validity of the proposed structure, points out a solution to advance information security defense, and provides some managerial recommendations to practitioners.

The first study examines the external hackers' behaviors and models a Bayesian game between a firm and two discrete types of hackers (domestic and international) based on the framework of Inspection Game. Pure Strategy Bayesian Nash Equilibriums (PSBNEs) are derived. Then, the continuous-type of hackers is extended to the basic model, and its PSBNEs

are also presented. Additionally, the paper incorporates information derived from external signals (e.g., newspapers or other media channels) to update the firm's prior beliefs of hacker types over time. The paper finds that a firm could prevent some domestic hackings but not effectively prevent international hackings. This is due to the cost of investigating data breaches by hackers in distant countries, as well as the perception by international hackers that they have a low risk of prosecution. Interestingly, there are some circumstances in which a firm will even choose to give up an investigation to avoid costs under the hackers' choice of hackings, no matter how severe a punishment it can impose. Moreover, when a firm observes a strong signal of domestic hackings in recent months, the firm will be able to effectively thwart some domestic hackers by imposing more severe penalties on them.

The second study is an empirical work and based on Hu et al. (2015) JMIS paper. It explores the other side of information security data breach, which is mainly due to the employees' noncompliance and ignorance of information security policy. This study aims to design and identify an incentive structure to better regulate the insider data breaches. Firstly, it examines how extrinsic incentives, Reward and Punishment, could help to enhance employees' compliant behavior. In addition, it also explores the impact of Collective Sanctions (Reward All and Punishment All) on employees' compliance. Due to the imperfect Intrusion Detection System (IDS) of a company, this study further investigates how a perceived low chance of detection influences employees' noncompliance. Lastly, it studies how Collective Sanctions and Detection working together to mitigate employees' noncompliant behavior.

Laboratory experiments with student subjects from Iowa State University were conducted. Four sequential experiments to study the aforementioned factors' impacts on information security policy compliance were developed. The main result, which is very significant, shows that individual reward and punishment with 100% detection is the best incentive structure among all other combinations. This result is in line with Andreoni et al. (2003, p. 901) saying "the absence of a reward is not equivalent to a punishment", as rewards and punishments are complementary to each other. Interestingly, another result shows individual reward is more effective than punishment, which seems to be contradictory to existing literature. However, paying additional rewards to motivate employees to put extra effort and time to follow the security policies seems to be more attractive for them compared with punishment. This could be illustrated by some giant IT companies' (like Google's) reward-oriented welfare package. Additionally, another result shows that collective sanctions have a spiral-downwards impact on cooperative compliance when interaction between subjects was not permitted. This result is consistent with the findings by Rand et al. (2009). Lastly, as expected, the perceived low chance of detection reduces the positive effects of reward as well as punishment. Hence, it is critical for a company to improve its IDS accuracy to achieve better compliance with a properly adapted reward and punishment incentive mechanism.

The third study is a conceptual work and introduces the breakthrough idea, Blockchain, the first native digital medium for securely transferring value over the Internet (Tapscott and Tapscott 2016). Furthermore, it relies on the Theory of Bounded Rationality to discuss how Blockchain technology can undermine the motivations of intruders in order to prevent information breaches. Particularly, it focuses on preventing intruders' monetary-gain motivation

from cashing out the stolen information assets, as such assets cannot be sold without appropriately transferring their ownership on the Blockchain ecosystems. This study further illustrates how the properties of distributed mechanism and immutability of Blockchain can greatly improve current information security defense against external hackers' attacks. In addition, since each unit of the content digitally stored on the Blockchain network can be programmed and auto-executed by the smart contract, and such execution is autonomous without middle parties, the properties of computational logic and peer-to-peer transmission thus can greatly prevent insider data breaches including both unintentional and intentional ones. Overall, the third study demonstrates how Blockchain can help to assist and advance information security defense.

CHAPTER 2. UNDERSTANDING DOMESTIC VS. INTERNATIONAL INTRUSION BEHAVIORS: A GAME-THEORETICAL MODEL

2.1. Introduction

The Internet has greatly benefited humanity by providing limitless and immediate information, communication, entertainment, and e-commerce to individuals, corporations, educational institutions, nonprofit organizations, and governments worldwide. Advances in technology have spawned gigabit networks, dramatically reducing the "virtual distance" between people and organizations. However, as the Internet has no borders and few regulations, its dark sides have been gradually revealed over time, especially with accelerated speed, making distance irrelevant (e.g., via mobile devices, LTE, etc.). The increasing globalizing influence of the Internet facilitates cross-business interconnectivity as well as data accessibility. However, it also brings a consequent increase in network vulnerability.

More and more aggressive hackings have occurred in recent decades. In fact, according to *The New York Times*, the F.B.I. ranks cybercrime as one of its top law enforcement activities, and the U.S. government has sharply increased its security budget to $14 billion (Granville 2015). In 2014, unknown hackers unlawfully obtained private photos of dozens of celebrities through the iCloud online storage service of Apple, Inc., violating the celebrities' privacy and shaking consumer confidence in Apple, Inc.'s network security, and online privacy in general. Also in 2014, Sony Pictures Entertainment was hacked by an unknown group, "Guardians of Peace," believed to be North Korean (Sanger et al. 2014). More recently, it was reported that some of President Obama's email correspondence was accessed by Russian hackers (Schmidt

and Sanger 2015). Hence, we cannot help wondering why firms, as well as government entities, are constantly facing cyberattacks. Is there an effective way to prevent hacking, and how can firms strategically respond to hackers?

The fact that countless hacking intrusions and destructive cyberattacks occurred in recent years without effective defenses from either business sectors or governments indicates that information security not only remains a crucial topic in information systems research, but is also essentially relevant to practices. A great deal of literature has been devoted to examining social norms and behavioral theories to explain how to prevent intrusion, especially that caused by internal staff. However, due to the limited availability of security data (e.g., number and extent of incidents), few new insights have been gained in recent years – certainly not sufficient to explain the increasing aggressiveness of hackers for the purposes of stealing trade secrets as well as political information. In fact, intrusion behavior is rarely studied through behavioral theories, because firms are afraid to release their security breach information and damage their brand equity. Without access to specific data on information security breaches, game theory becomes the logical approach to study the interplays between firms and hackers. It provides powerful tools that allow us to model a sophisticated hacker who knows how to gain access as well as what defense strategies are used by a firm, and can adjust his attack strategies accordingly. Though game theory has been frequently criticized by psychologists for its assumptions (e.g., rationality), it is still one of the most useful approaches to studying the interaction phenomena to predict the steady stage of game between players, without full details. Moreover, abstract modeling permits game theory to explain a set of phenomena, rather than merely isolated

incidents. This more complete picture can enhance our ability to understand why cyber-intrusions are so pervasive.

In this study, we proposed a Bayesian game for modeling intrusion behavior to capture the interplay between a hacker's intrusion and a firm's subsequent investigation. Particularly, we differentiated international hackers from domestic ones to explain the increasing number of international hackings. We further incorporated the external "signals" (e.g., newspaper reports) which organizations may use to adjust their best response strategies to different types of hackers. The results of our model caution the firm that it is unlikely to prevent international hackings and should conserve its resources to avoid futile spending. Fortunately, under certain conditions, a firm could effectively deter domestic hackings to minimize losses.

2.2. Review of the Literature

Our work is closely related to Cavusoglu et al. (2005). They constructed a Nash game with complete information based on the framework of Inspection Game in econometric literature (Fudenberg and Tirole 1991). In their paper, the firm is modeled as "the principal" to choose "Investigate" or "Not Investigate," and hackers are "the agent" to choose "Hack" or "Not Hack." The hacker gains a benefit if intrusion occurs without the firm's inspections; otherwise, the hacker receives a penalty when the firm investigates the transaction activities. Additionally, the firm must pay the cost of labor for the investigation, but could save a fraction of damage prevented or recovered when an intrusion is detected. Cavusoglu et al. (2005) found a mixed-strategy Nash equilibrium which is the probability profile for the firm to investigate and the hacker to hack. However, as debated in game theory literature, mixed- strategy equilibrium is

difficult to interpret, since it implies that both the firm and the hacker commit themselves to using a random device to play the game (Osborne and Rubinstein 1994).

In reality, hackers often strategically choose those targets which are easy to break into or which yield a better payoff, although a firm may have no idea when and how the intrusion will occur for a single play of an incident (Cremonini and Nizovtsev 2009). Hence, in our model we focus on pure-strategy Nash equilibriums, rather than mixed-strategy equilibriums. Additionally, to our knowledge, the existing literature (Alpcan and Basar 2006; Bloem et al. 2006; Çakanyıldırım et al. 2009; Cavusoglu et al. 2005; Lin et al. 2009; Liu et al. 2006; Nguyen et al. 2009; Patcha and Park 2004) arbitrarily treat all hackers equally, which is not accurate in our virtual world.

As aforementioned, advancing Internet technology brings people much closer than before, and hacking overseas becomes a commonplace activity. In fact, *The New York Times* reported that since 2013, an international cybercriminal group has stolen up to $1 billion from more than 100 banking and financial institutions in 30 different countries around the world. More concerning, these cyberattacks continued for two years without detection by banks, regulators, or law enforcement (Sanger and Perlroth 2015). As hackers come from different geographical regions, the level of control over such attacks varies accordingly. Furthermore, equipped with sophisticated technology (e.g., IP masking, anonymous surfing, etc.), hackers can hide their IP addresses from detection, which increases the difficulty of being caught by firms. In other words, there is no effective deterrent due to the increased difficulty in identifying and

stopping hackers. Therefore, we proposed a novel model differentiating *international* hackers from *domestic* ones, to illustrate the distinct intrusion behaviors of each group.

The broader area of this paper falls under non-cooperative games in the concept of econometric literature (Fudenberg and Tirole 1991). In the context of cyber-security, much research has been done in computer science as well as computer engineering communities. Liu et al. (2006) also built their model based on inspection games and examined the interaction between pairs of attacking and defending nodes, using a Bayesian formulation. Each node of a flat ad hoc network was treated either as malicious and regular users or defenders of network administrators. Furthermore, they developed dynamic Bayesian game intrusion-detection algorithms and designed a hybrid detection mechanism. Their paper aims to increase the precision of intrusion detection as well as the energy efficiency of defenders. Our paper differs from their research in considering the business components (i.e., costs of monitoring intrusions, costs of investigation, costs of lawsuits, investment of time, etc.) and different impacts of distinct types of hackers.

In addition, Patcha and Park (2004) modeled intrusion detection in mobile ad-hoc networks by adapting the signaling game in the multi-stage dynamic non-cooperation frameworks. Alpcan and Basar (2006) modeled the interactions between malicious attackers and their targets' intrusion detection systems using a stochastic (Markov) game. They captured the operation of the intrusion- detection sensor system using a finite-state Markov chain and naïve Q-learning (Bertsekas et al. 1995) to find the best strategies. Nguyen et al. (2009) adopted the "fictitious play" game framework to model the interplay between hackers and defenders as a

sequence of a non-zero game. Lin et al. (2009) viewed the interactive behavior between the hacker and the defender as information warfare and developed a tree diagram based on game theory. In spite of the complex games used in previous literature, those researchers only focused on the classifications of malicious and regular users, as well as evaluating the defensive mechanisms of systems. They did not consider the large number of hackers nor the diversity in their intrusion behaviors.

From the cost perspective, Bloem et al. (2006) developed an algorithm for optimal allocation of a system administrator's time available for responding to attacks, based on a non-cooperative non-zero sum game. Çakanyıldırım et al. (2009) examined the investigation costs, damage, and occurrence probabilities of intrusion in the presence of multiple alarm types. Nevertheless, they did not differentiate the impact of different types of hackers nor consider the differences in the costs of preventing intrusions.

The following section presents our basic Bayesian game model, and the Pure Strategy Bayesian Nash Equilibriums (PSBNEs), as well as our insights, are provided. In section 4, a more general Bayesian game is characterized. In section 5, a Bayesian game with learning of external signals is constructed. We interpret the PSBNEs, particularly when switching strategies under certain conditions of the signal effects in comparison with the basic model. Finally, we present our conclusions in section 6.

2.3. The Basic Bayesian Game Model

Abstracted from real-life scenarios, especially from newspaper reports, we assume that hackers comprise two types – $\theta_H = \{Domestic, International\}$ – which reflects the modern trend of both geographical types of hackings. Both types of hackers can choose to Hack (H) or Not Hack (NH). Therefore, the hacker's strategy space is: $S_H = \{(H,H), (H,NH), (NH,H), (NH,NH)\}$, where the first element of the pair is the strategic action chosen by *Domestic* hackers, and the second element is the strategic action chosen by *International* hackers. Meanwhile, the firm can choose to Investigate (I) or Not Investigate (NI). Accordingly, the firm's strategy space is $S_F = \{I, NI\}$. The payoff matrices for both players with two types of hackers are given in Table 1:

Table 1.(a) Payoff of $\theta_H = Domestic$

	H	NH
I	$(-c^D - (1-\phi)d, \mu - \beta^D)$	$(-c, 0)$
NI	$(-d, \quad \mu)$	$(0, 0)$

Table 1.(b) Payoff of $\theta_H = International$

	H	NH
I	$(-c^I - (1-\phi)d, \mu - \beta^I)$	$(-c, 0)$
NI	$(-d, \quad \mu)$	$(0, 0)$

As shown in Table 1, the firm pays c, where $c > 0$, for the cost of monitoring one incident, and c may be sufficiently small, depending on the policies employed by the firm (e.g., fully automated monitoring, manual monitoring, or semi-automated monitoring). It costs the firm c^D and c^I to investigate an intrusion caused by a *domestic* and *international* hacker, respectively. The aggregate investigation cost c^D and c^I includes the monitoring cost (i.e., c), payment to investigators, efforts spent to catch hackers after hackers were detected, etc. The investigation of an *international* hacking is complex and time-consuming, so it is understandable that it is also much more costly than that of a *domestic* hacking (i.e., $c^I \gg c^D \gg c$). In addition, successfully investigating an international cyberattack almost always requires assistance from the government, e.g., the F.B.I.

For example, Anthem, one of the nation's largest health insurers, was penetrated in January 2015 by hackers who gained the personal information, including Social Security numbers, of 80 million Anthem customers and employees (Mathews and Yadron 2015). Anthem hired F.B.I. cyber-experts and the cyber-security firm, Mandiant, to help investigate the intrusion, and it took several months to identify the hackers' origins (China). The cost of the investigation was massive. Furthermore, we denote that damage to the firm by an undetected intrusion is $d > 0$. It varies among different firms and can be estimated in the risk assessment from a firm's IT department. Additionally, through the investigation process, a firm may be able to recover a portion of the value of the damage caused by intrusions. For example, a firm can hire technology experts to recover at least partial data from the hard drives which were compromised by hackers. Therefore, we denote the fraction of damage recovered by an

investigation process as ϕ, where $\phi \in [0,1]$. ϕ could be obtained from a consulting firm's IT department or external technology experts, based on historical cases.

Suppose in one incident, a hacker gains the benefit μ from breaching the firm's database without being caught, where $\mu > 0$. It is reasonable to assume μ is the same with either *domestic* or *international* hackers. In addition, the cost of a hacker intrusion is the same with different attacked firms, since we consider only one type of firm (e.g., the equal level of defender systems). If the intrusion is detected, *domestic* and *international* hackers incur the expected penalty of β^D and β^I, respectively. The expected penalty β^D and β^I mainly refers to legal prosecution, but also could be social humiliation.

Because of the difficulty in catching and prosecuting international cybercriminals, the expected penalty on a *domestic* hacker is much heavier than that on an *international* one (i.e., $\beta^D \gg \beta^I > 0$), although the publicly stated penalty could be the same for both types of hackers (e.g., imprisonment). For instance, the F.B.I announced rewards of up to $100,000 for information leading to the arrest of five international hackers (Bisson 2013). Accordingly, the net benefits of hackers to attack and be detected is $\mu - \beta^D$ and $\mu - \beta^I$ for *domestic* and *international* hackers, respectively. In contrast to Cavusoglu et al. (2005), we put no further restrictions on $\mu - \beta^D$ or $\mu - \beta^I$, since μ could be quite large. As mentioned earlier, $1 billion from 100 banking and financial institutions was stolen by hackers, but few of them have been arrested. Hackers, especially international ones, know that they are unlikely to be caught; therefore, arbitrarily assuming $\mu - \beta^D \leq 0$ and $\mu - \beta^I \leq 0$ is not realistic.

Let q be the prior of the firm to believe that the hackers are *domestic* and, thus, $1 - q$ is the firm's belief that the hackers are *international*. This prior q can be easily obtained from the firm's historical intrusion data by reviewing the percentage of *domestic* hackings over all detected intrusions. We model both the firm and the hackers as strategically choosing their actions simultaneously, at a given point in time. Figure 1 illustrates the extensive form of our basic Bayesian game. In the figure, the hacker's type is the hacker's private information, and "Nature" determines the type of hackers. The firm does not know which specific type of hackers it is facing, since the firm is in a single information set. Both payoffs of the firm and the hackers are common knowledge. The objective of both the firm and the hackers is to maximize their expected payoffs. To solve the game, its normal form is also given in Table 2.

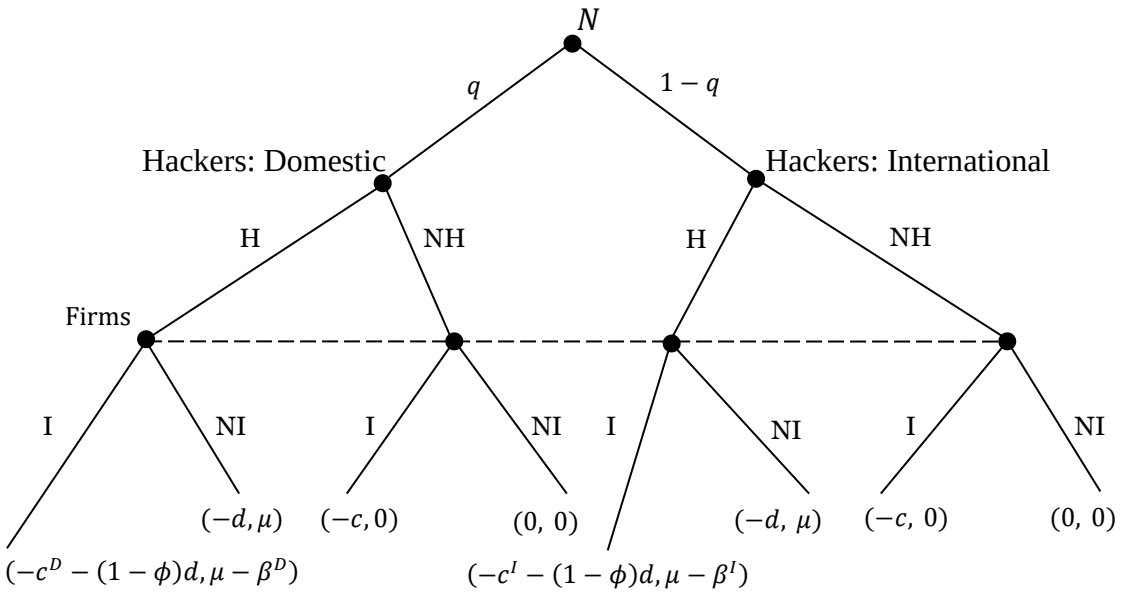

Figure 1. Extensive Form of Basic Bayesian Game

Table 2. Normal Form of Two Types of Hackers Bayesian Game

	(H, H)	(H, NH)	(NH, H)	(NH, NH)
I	$\begin{pmatrix} U_F(I\|s_H=(H,H)), \\ (\mu-\beta^D, \mu-\beta^I) \end{pmatrix}$	$\begin{pmatrix} U_F(I\|s_H=(H,NH)), \\ (\mu-\beta^D, 0) \end{pmatrix}$	$\begin{pmatrix} U_F(I\|s_H=(NH,NH)), \\ (0, \mu-\beta^I) \end{pmatrix}$	$(-c, \quad (0,0))$
NI	$(-d, \quad (\mu,\mu))$	$(q(-d), \quad (\mu,0))$	$((1-q)(-d), \quad (0,\mu))$	$(0, \quad (0,0))$

Where, $\begin{cases} U_F(I|s_H=(H,H)) = q[c^I - c^D] - [c^I + (1-\phi)d] \\ U_F(I|s_H=(H,NH)) = q[c - c^D - (1-\phi)d] - c \\ U_F(I|s_H=(NH,NH)) = q[c^I - c + (1-\phi)d] - [c^I + (1-\phi)d] \end{cases}$

Solving the normal form in Table 2 yields the following Proposition 1:

Proposition 1. *The Pure Strategy Bayesian Nash Equilibriums for the firm and two discrete types of hackers are as follows, where* $\{\cdot,(\cdot,\cdot)\}$ *denotes the equilibrium strategy profiles, and the first element in the braces is the strategy action chosen by the firm, and the second one is for the hackers.*

$$Play\ \{I,(H,H)\},\ if \begin{cases} \mu-\beta^I > \mu-\beta^D > 0 \\ q > \frac{c^I-\phi d}{c^I-c^D} \end{cases} \quad (1)$$

$$Play\ \{NI,(H,H)\},\ if \begin{cases} \mu-\beta^I, \mu-\beta^D \in \mathbb{R} \\ q < \frac{c^I-\phi d}{c^I-c^D} \end{cases} \quad (2)$$

$$Play\ \{I,(NH,H)\},\ if \begin{cases} \mu-\beta^I > 0,\ \mu-\beta^D < 0 \\ q > \frac{c^I-\phi d}{c^I-\phi d-c} \end{cases} \quad (3)$$

Proposition 1 provides us three distinct strategy profiles which the firm and the hackers adopted in the steady stage. PSBNE (1) indicates that if the penalties in relation to the hackers' benefits are not heavy enough ($\mu-\beta^I > \mu-\beta^D > 0$), and the firm believes that there are large

enough proportions ($q > \frac{c^I - \phi d}{c^I - c^D}$) of *domestic* hackers, the firm will choose to investigate and the hackers will certainly choose to hack for better payoff. PSBNE (2) shows that if the firm perceives that the proportion of *domestic* hackers is small enough ($q < \frac{c^I - \phi d}{c^I - c^D}$), the firm will choose to not investigate, no matter which type of hackers and which penalty/benefit parameters.

This counterintuitive finding can be explained as follows: When the deterrents are severe ($\mu - \beta^D < \mu - \beta^I < 0$), hackers firstly choose to not hack to avoid negative net benefits; then the firm secondly stops investigating intrusion behaviors due to its cost c. Next, the hackers will again choose to attack. Eventually, the steady strategy for both players is $\{NI, (H, H)\}$. Finally, PSBNE (3) matches our intuitions. When only *international* hackers can enjoy positive net benefit, they will choose to hack, but *domestic* hackers will stop hacking to avoid their negative net benefit; meanwhile, the firm will choose to investigate when it believes there are large enough numbers ($q > \frac{c^I - \phi d}{c^I - \phi d - c}$) of *domestic* hackers. There may be several temporary stages in the game when hackers will choose to not hack and the firm's investigations are in vain, but those stages are not stable as the game is being played by both rational players. According to Rational Expectations Theory (Muth 1961), both the firm and the hackers will be stuck in the aforementioned pure-strategy Bayesian Nash equilibriums and will have no incentives to deviate.

Cavusoglu et al. (2005) assumed that the firm's cost to investigate is not higher than the retrieved benefits under the detected intrusion. However, in our model, we relax this assumption and allow $c^I - \phi d$ and $c^D - \phi d$ to be any real number. Hence, the cost of investigating both *domestic* and *international* hackers could be greater or less than the firm's retrieved benefits

from the detected damage. In some situations, the firm's retrieved benefits from detection can be greater than its investigation cost, especially when the damage is easy to recover and the hackers are easy to catch. On the other hand, the firm has to chase hackers due to the pressure from customers and legal requirements, even though their investigation costs could be enormous. Like the aforementioned Anthem case, retrieved value from the damage is much smaller than the resources Anthem spent on the investigations.

The corollary below follows from Proposition 1:

Corollary 1. *The equilibriums of our intrusion-behavior game model indicate that the firm is unlikely to effectively prevent international hackers as long as the monitor cost* $c > 0$*, no matter how severe the expected punishment.*

Corollary 1 provides compelling theoretical support for media reports that both firms and governments are constantly facing international hackings. The firm may be able to stop a *domestic* cyberattack if the number of *domestic* hackers is large enough ($q > \frac{c^I - \phi d}{c^I - \phi d - c}$) and the expected penalty is severe enough on the *domestic* hackers (e.g., punishments from domestic law enforcement). This result delineates the boundary of the General Deterrence Theory proposed by Straub Jr (1990), which argues that unwanted behavior could be deterred when *perceptions* of the certainty and severity of punishment for IS misuse is increased. For those rational *domestic* hackers who *perceive* the certainty and severity of punishment (i.e., expected penalty) is severe enough, they will choose to not hack. However, rational *international* hackers will continually choose to hack, no matter how severe the expected penalty is. This finding supports President

Obama's recently announced cybersecurity legislative proposal that government must do more to support the private sector in establishing strong regulation and a better legal environment (Secretary 2015).

Furthermore, when the cost of catching *international* hackers is less than the damage recovered from the investigation process ($c^I - \phi d < 0$), in spite of the firm's beliefs of the hackers' type, hackers will always choose to attack, even with the firm's investigations, as long as they can gain a positive net benefit (PSBNE (1)). By comparing the PSBNE (1) and (2), we can see that hackers will always choose to hack, and the firm's decision-making depends merely on their prior beliefs of hackers' types, as long as $c^I - \phi d > 0$. Another interesting finding is that punishment for hackers is not "the more severe, the better." As we can see from the process of obtaining PSBNE (2), severe punishment can only deter hacks temporarily, and hackers will continually choose to hack when firms change their strategy to not investigate. Therefore, for the U.S. government to enact legislation to enhance cybersecurity, it is necessary to consider the firm's cost parameters, rather than to arbitrarily set an unrealistically high standard for punishment.

2.4. The Continuous-Type Hacker Bayesian Game Model

Classifying hackers as *domestic* and *international* is intuitive, but Russian and European hackers have distinct impacts on American firms, as well as American firms' retaliations. One critical reason for this may be diminished legal power over a great distance. American legal proceedings may more easily reach Europe than Russia. Therefore, a more general model is to allow hackers to have continuous type θ_H, which can be interpreted as the "distance" between

the firm and the hacker. Here, we define the "distance" as the level of difficulty involved for the firm to catch the hacker. The abstract meaning of "distance" is a multi-dimensional concept, which is composed of the geographical distance between the firm and the hacker, the distance in legislative power between law enforcement and the hacker, technology barriers between an ordinary firm and a sophisticated hacker, and so on.

Without loss of generality, we further normalize hacker's type $\theta_H \in [0,1]$. We further assume that the cost to the firm to investigate the intrusion behaviors is a function of θ_H, and so is the penalty of hackers to intrude. Based on our definition of "distance," it makes sense that with the increasing difficulty of catching hackers, the cost of investigating them will be increased, but the expected penalty on them will be decreased. Therefore, let a monotone increasing function $w(\theta_H)$ be the total cost, including the monitor cost c, for the firm to investigate hackers, and another monotone decreasing function $g(\theta_H)$ be the expected penalty on hackers for intrusion. In addition, we define $\bar{\theta}_H$ as the marginal hackers, whose utilities are indifferent between NOT hacking and hacking. Because $g(\theta_H)$ is monotone decreased, the hacker's payoff under firm's investigation $U_H(\theta_H|s_F = I) = (\mu - g(\theta_H)|s_F = I)$ is thus a monotone increasing function. As Figure 2 indicates, it will be better for hackers to not hack when their types are less than $\bar{\theta}_H$, but to hack if otherwise. Therefore, for a given type of hacker, there is the following payoff matrix (Table 3) and expected utilities for both the firm and the hackers, where $f(\theta_H)$ denotes the probability density function over the hacker's type $\theta_H \in [0,1]$.

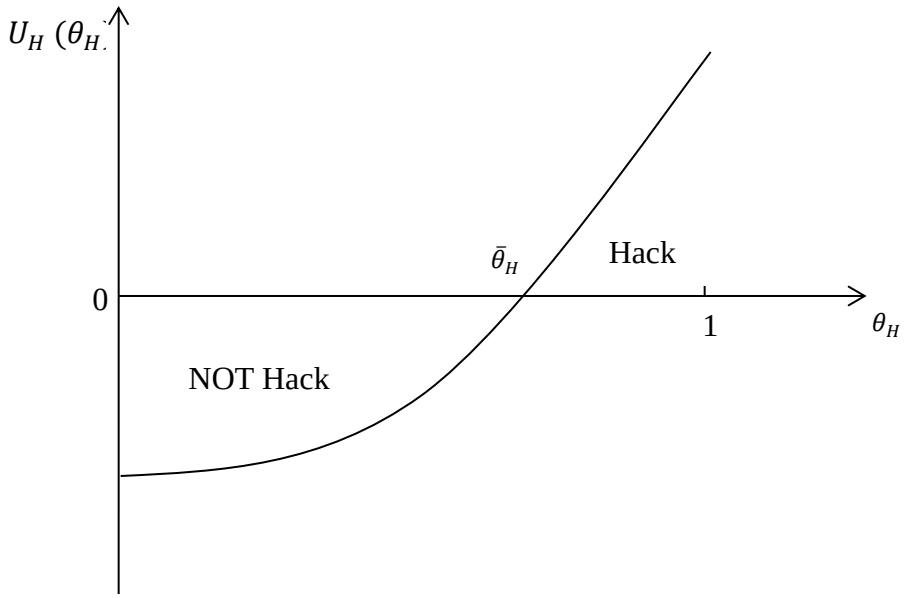

Figure 2. Marginal Hackers

Table 3. Continuous-Type Payoff Matrix

	$H(\theta_H)$	$NH(\theta_H)$
I	$\left(-w(\theta_H)-(1-\phi)d, \mu-g(\theta_H)\right)$	$(-c,0)$
NI	$(-d,\mu)$	$(0,0)$

$$U_F(\theta_H|s_F=I)=\int_0^{\bar{\theta}_H}-cf(\theta_H)\,d\theta_H+\int_{\bar{\theta}_H}^{1}(-w(\theta_H)-(1-\phi)d)f(\theta_H)\,d\theta_H$$

$$U_F(\theta_H|s_F=NI)=\int_0^{\bar{\theta}_H}0f(\theta_H)\,d\theta_H+\int_{\bar{\theta}_H}^{1}(-d)f(\theta_H)\,d\theta_H=\int_{\bar{\theta}_H}^{1}(-d)f(\theta_H)\,d\theta_H$$

$$U_H(\theta_H|s_F=I)=\begin{cases}0, & \theta_H\le\bar{\theta}_H\\ \mu-g(\theta_H), & \theta_H>\bar{\theta}_H\end{cases}$$

$$U_H(\theta_H|s_F=NI)=\begin{cases}0, & \theta_H\le\bar{\theta}_H\\ \mu, & \theta_H>\bar{\theta}_H\end{cases}$$

In order to obtain the Pure Strategy Bayesian Nash Equilibriums, we need to further specify the function forms for both $w(\theta_H)$ and $g(\theta_H)$. Due to the skewed nature of the firm's cost function, as well as the penalty function on the hackers, let $w(\theta_H) = c + \gamma_c \theta_H^2$ and $g(\theta_H) = \beta - \gamma_\beta \theta_H^2$, where $\gamma_c > 0$ and $\gamma_\beta > 0$. It is worthwhile to note that c is the monitor cost (as well as the minimum cost) for the firm to catch the hackers, and β is the maximum expected penalty on the hackers for intrusion. Furthermore, we assume that the hacker's types are uniformly distributed between zero and one (i.e. $f(\theta_H) = 1$).

Although the hacker's type is continuous, the game has infinite discrete strategy space. For notational convenience, we index $\bar{\theta}_H$ as $0 = \bar{\theta}_H^{0\%} < \cdots < \bar{\theta}_H^k < \cdots < \bar{\theta}_H^{100\%} = 1$. To illustrate, $(\bar{\theta}_H^k : 1 - \bar{\theta}_H^k)$ represents the hacker's strategy space as $(NH, \dots, NH, H, \dots, H)$ over the continuous type $\theta_H \in [0, 1]$; in this discrete infinite set of the hacker's strategy space, k hackers will choose "*NH*," and $(1 - k)$ hackers will choose "*H*," where k is a percentage between 0% and 100%. Using this newly introduced notation, we can get the normal form of the Bayesian game with continuous types of hackers as follows in Table 4.

Table 4. Normal Form of Continuous Types of Hackers Bayesian Game

	$(\bar{\theta}_H^{0\%} : 1-\bar{\theta}_H^{0\%})$	...	$(\bar{\theta}_H^{k} : 1-\bar{\theta}_H^{k})$	...	$(\bar{\theta}_H^{100\%} : 1-\bar{\theta}_H^{100\%})$
I	$\begin{pmatrix} -\left[c+(1-\phi)d+\frac{1}{3}\gamma_c\right], \\ (\mu-\beta+\gamma_\beta\theta_H^2, \dots, \mu-\beta+\gamma_\beta\theta_H^2) \end{pmatrix}$	...	$\begin{pmatrix} U_F(\theta_H \mid s_F = I), \\ (0, \dots, \mu-\beta+\gamma_\beta\theta_H^2) \end{pmatrix}$	...	$(-c, \quad (0, \dots, 0))$
NI	$(-d, \quad (\mu, \dots, \mu))$	...	$(U_F(\theta_H \mid s_F = NI), (0, \dots, \mu))$	...	$(0, \quad (0, \dots, 0))$

Where, $\begin{cases} U_F(\theta_H \mid s_F = I) = \frac{1}{3}\gamma_c\bar{\theta}_H^3 + (1-\phi)\bar{\theta}_H d - \left[c+(1-\phi)d+\frac{1}{3}\gamma_c\right] \\ U_F(\theta_H \mid s_F = NI) = (\bar{\theta}_H - 1)d \\ U_H(\theta_H \mid s_F = I) = \begin{cases} 0, & \theta_H \le \bar{\theta}_H \\ \mu-\beta+\gamma_\beta\theta_H^2, & \theta_H > \bar{\theta}_H \end{cases} \\ U_H(\theta_H \mid s_F = NI) = \begin{cases} 0, & \theta_H \le \bar{\theta}_H \\ \mu, & \theta_H > \bar{\theta}_H \end{cases} \end{cases}$

Solving the continuous type of hackers' Bayesian game yields the following Proposition 2:

Proposition 2. *The Pure Strategy Bayesian Nash Equilibriums for the firm and continuous-type of hackers are as follows, where* $\{\cdot, (\cdot : \cdot)\}$ *denotes the equilibrium strategy profiles, and the first element in the braces is the strategy action chosen by the firm, and the second one is for hackers. Additionally, for notational convenience, the pairs in parentheses are the proportions for hackers to choose NOT hack and hack, respectively.*

$$Play\ \{I, (0:1)\},\ if \begin{cases} \mu > \beta \\ \phi > \frac{3c+\gamma_c}{3d} \end{cases} \tag{4}$$

$$Play\ \{NI, (0:1)\},\ if \begin{cases} \mu-\beta \in \mathbb{R} \\ \phi < \frac{3c+\gamma_c}{3d} \end{cases} \tag{5}$$

$$Play\ \{I, (\bar{\theta}_H^* : 1 - \bar{\theta}_H^*)\},\ where\ \bar{\theta}_H^* = \sqrt{\frac{\beta-\mu}{\gamma_\beta}},\ if \begin{cases} 0 < \beta - \mu < \gamma_\beta \\ \phi > \dfrac{\left[1-\left(\frac{\beta-\mu}{\gamma_\beta}\right)^{\frac{3}{2}}\right]\gamma_c+3c}{3\left[1-\left(\frac{\beta-\mu}{\gamma_\beta}\right)^{\frac{1}{2}}\right]d} \end{cases} \quad (6)$$

As expected, Proposition 2 is consistent with Proposition 1, but also provides some new insights for the firm's decision-making. PSBNE (4) shows that if the firm can recover a large enough proportion ($\phi > \frac{3c+\gamma_c}{3d}$) of their damage, and if hackers' benefits are greater than the maximum expected penalty, the firm will choose to investigate and all types of hackers will choose to attack. PSBNE (5) indicates that if the firm believes their retrieved proportion of value over the damage is low enough ($\phi < \frac{3c+\gamma_c}{3d}$), hackers will choose to hack and the firm will give up investigation, no matter the hackers' net benefits. Although it is counterintuitive and implausible behavior for the firm to stop investigating, it is also irrational to spend more money to investigate than the value received in return.

PSBNE (6) is the most interesting and useful finding. It states that when the net expected penalty on hackers is in a certain range ($0 < \beta - \mu < \gamma_\beta$), and the fraction of damage recovered is large enough ($\phi > \left\{\left[1-\left(\frac{\beta-\mu}{\gamma_\beta}\right)^{\frac{3}{2}}\right]\gamma_c + 3c\right\} \Big/ 3\left[1-\left(\frac{\beta-\mu}{\gamma_\beta}\right)^{\frac{1}{2}}\right]d$), the firm will choose to investigate and a proportion ($\bar{\theta}_H^* = \sqrt{\frac{\beta-\mu}{\gamma_\beta}}$) of hackers will choose to stop attacking. This equilibrium not only instructs the firm on how to prevent intrusion behaviors with respect to some parameters, but also demonstrates the specific percentage of hackers the firm could deter. Recall the convex function form we defined for the expected penalty on hackers as $g(\theta_H) = \beta - \gamma_\beta \theta_H^2$, where γ_β can be interpreted as a deterrence decay coefficient. The smaller the value

of γ_β, the more severe the punishment on the hackers. As we can see from the PSBNE (6), γ_β cannot take the value of zero. In other words, it is not always effective to prevent intrusion behavior by arbitrarily setting a super-heavy penalty, regardless of the firm's cost parameters, which also confirms the previous finding in the two-type hacker's game.

Careful readers may wonder if we can allow $\beta - \mu \geq \gamma_\beta$, which will lead to $\bar{\theta}_H^* \geq 1$. In this case, it seems that all types of hackers will choose to not hack. But similar to the analysis of the two-type game, the firm will choose to stop investigating due to its cost $c > 0$. Therefore, it will not form a Nash equilibrium. However, if the monitor cost (e.g., fully automated) can be negligible ($c = 0$), it is possible for the firm to prevent all hackers' intrusions under severe punishment ($\beta - \mu \geq \gamma_\beta$). Hence, matching our intuition, the most practical advice to the firm is to reduce monitoring cost and increase the precision of automated detection in order to reduce manual detection cost.

2.5. Bayesian Game with Learning of External Signal

Learning from past experience is beneficial for humans as well as firms; lessons from peers or others are even more useful for a firm's decision-makers to predict/prevent future events (i.e., intrusion behaviors in our context). For the sake of parsimony and intuition, we only discuss the two types of hackers in this section. As an illustration, suppose Walmart and Target are repeatedly facing domestic hacking (say, 30%) and international hacking (say, 70%). Unfortunately, *The New York Times* reports that Target's network was attacked by some international hackers (Abrams 2014). If the CIO of Walmart reads the newspaper article, it is not unreasonable to assume that she will decide that Walmart needs to update its beliefs about the

percentage of international hackers (say from 70% to 80%) that will attack Walmart in the near future. This scenario can be reflected by Figure 3.

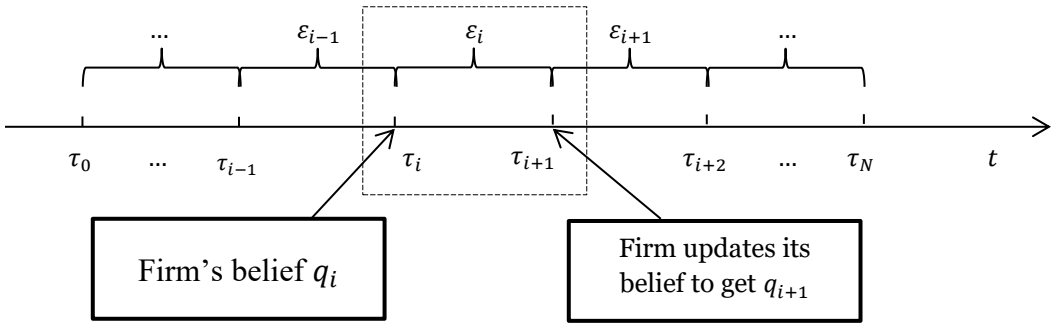

Figure 3. Updating the Firm's Belief with Respect to External Signal

At a given time τ_i, the firm can obtain its belief q_i from reviewing its own historical data. After observing the external signal ε_i (e.g., newspapers or other media), which indicates the strength/frequency of *domestic* hacking over all intrusions that occurred during time period (τ_i, τ_{i+1}), the firm can update its belief to get q_{i+1}. It is worthy to note that ε_i is a random variable, depending on time, and can be distributed as uniform, normal, Poisson, etc. In this study, we do not specify the particular function form for ε_i; instead, we treat it as a stochastic variable. Furthermore, we normalize $\varepsilon_i \in [0, 1]$. Due to the restrictions of $q_i, q_{i+1} \in [0, 1]$, we assume $q_{i+1} = (1 - \alpha)q_i + \alpha\varepsilon_i$, where α is the perceived signal impact factor representing the internalizing effects of external information into the firm's prior beliefs about the hacker's type. Although the game between the firm and hackers is played repeatedly, we can still focus on the game stage i and $i + 1$ to study the intrusion behaviors, because no discount factors with respect to the payoffs of the players are introduced in our model. Therefore, for a one-shot simultaneous

game at stage $i+1$, we can replace q_i with q_{i+1} to get new pure-strategy Bayesian Nash equilibriums as follows:

$$Play\ \{I,(H,H)\},\ if\ \begin{cases} \mu-\beta^I>\mu-\beta^D>0 \\ q_i>\left(\frac{1}{1-\alpha}\right)\frac{c^I-\phi d}{c^I-c^D}-\left(\frac{\alpha}{1-\alpha}\right)\varepsilon_i \end{cases} \tag{7}$$

$$Play\ \{NI,(H,H)\},\ if\ \begin{cases} \mu-\beta^I,\ \mu-\beta^D\in\mathbb{R} \\ q_i<\left(\frac{1}{1-\alpha}\right)\frac{c^I-\phi d}{c^I-c^D}-\left(\frac{\alpha}{1-\alpha}\right)\varepsilon_i \end{cases} \tag{8}$$

$$Play\ \{I,(NH,H)\},\ if\ \begin{cases} \mu-\beta^I>0,\ \mu-\ \beta^D<0 \\ q_i>\left(\frac{1}{1-\alpha}\right)\frac{c^I-\phi d}{c^I-c-\phi d}-\left(\frac{\alpha}{1-\alpha}\right)\varepsilon_i \end{cases} \tag{9}$$

PSBNE (7)-(9) is also consistent with Proposition 1. However, by comparing the conditions of PSBNE (1)-(3) and current equilibriums, we can characterize the impacts of external signals on the steady strategy profiles which will be played out by the firm and the hackers over time. Accordingly, Proposition 3 is as follows:

Proposition 3. *When the External Signal ε_i falls to a certain interval, the Pure Strategy Bayesian Nash Equilibrium will switch from one to another over time,*

(i) *In stage i, if the PSBNE $\{I,(H,H)\}$ occurs and $\varepsilon_i\in\left[0,\ \frac{c^I-\phi d}{\alpha(c^I-c^D)}-\frac{1-\alpha}{\alpha}q_i\right)$, the PSBNE will switch to $\{NI,(H,H)\}$ in stage $i+1$.* (10)

(ii) *In stage i, if the PSBNE $\{NI,(H,H)\}$ occurs and $\varepsilon_i\in\left(\frac{c^I-\phi d}{\alpha(c^I-c^D)}-\frac{1-\alpha}{\alpha}q_i,1\right]$, the PSBNE will switch to $\{I,(H,H)\}$ in stage $i+1$ as long as $\mu-\beta^I>\mu-\beta^D>0$.* (11)

(iii) *In stage i, if the PSBNE $\{I,(NH,H)\}$ occurs and $\varepsilon_i\in\left[0,\ \frac{c^I-\phi d}{\alpha(c^I-\phi d-c)}-\frac{1-\alpha}{\alpha}q_i\right)$, the previous PSBNE $\{I,(NH,H)\}$ will disappear in stage $i+1$* (12)

(iv) *In stage i, if $\varepsilon_i \in \left(\frac{c^I-\phi d}{\alpha(c^I-\phi d-c)}-\frac{1-\alpha}{\alpha}q_i, 1\right]$, a new PSBNE will emerge as $\{I,(NH,H)\}$ in stage $i+1$ as long as $\mu-\beta^I>0, \mu-\beta^D<0$.* (13)

Proposition 3 implies that under a certain external signal strength, the equilibrium strategy profiles of the firm and the hackers will not be stable when the game is played repeatedly over time. Condition (10) indicates that when the signal strength is small enough ($\varepsilon_i \in \left[0, \frac{c^I-\phi d}{\alpha(c^I-c^D)}-\frac{1-\alpha}{\alpha}q_i\right)$), the firm will choose to forgo investigations in the following stage, but the hackers will keep hacking. In other words, when the firm perceives a strong signal of *international* hackings, the firm will choose to not investigate to save costs. Condition (11) states that when hackers can receive positive net benefits, and the external signal is large enough ($\varepsilon_i \in \left(\frac{c^I-\phi d}{\alpha(c^I-c^D)}-\frac{1-\alpha}{\alpha}q_i, 1\right]$), the firm will choose to investigate in the following stage and the hackers will keep hacking.

This finding is counterintuitive; however, when a strong signal indicates more *domestic* hackers, the firm is better off investigating to catch hackers, as well as recover some damages to reduce losses, even if the hackers will gain positive net benefits. Interestingly, condition (12) shows that when the external signal is small enough ($\varepsilon_i \in \left[0, \frac{c^I-\phi d}{\alpha(c^I-\phi d-c)}-\frac{1-\alpha}{\alpha}q_i\right)$), the previous PSBNE $\{I,(NH,H)\}$ will disappear. In the previous stage, the firm chose to investigate and *domestic* hackers chose to not hack due to the severe deterrence ($\mu-\beta^I>0, \mu-\beta^D<0$). However, when the firm observes there will be a large proportion of *international* hackings, the firm will choose to stop investigation to save costs and *domestic* hackers will switch back to attack; accordingly, equilibrium cannot converge. The most useful finding for the firm is

condition (13). It illustrates that when the firm perceives a strong signal of *domestic* hackings ($\varepsilon_i \in \left(\frac{c^I-\phi d}{\alpha(c^I-\phi d-c)} - \frac{1-\alpha}{\alpha} q_i, 1\right]$), the firm will be able to effectively prevent *domestic* cyberattacks in the following stage, as long as *domestic* hackers receive heavy punishment$\mu - \beta^I > 0, \mu - \beta^D < 0$.

By analyzing the equilibrium switching from time to time, the external signal ε_i is unlikely to help the firm to effectively prevent *international* hackers, no matter how strong or weak the signal. This finding is consistent with Corollary 1, since the external signal ε_i essentially updates the firm's prior belief of the hackers' type. However, with the help of external signals, the firm could learn how to respond strategically to the hackers. Condition (13) indicates that the firm could learn from peers' experience to prevent *domestic* hackers in certain stages. Condition (10) advises the firm to stop investigation to avoid unnecessary spending. On the other hand, condition (11) recommends that the firm investigate to reduce losses or recover partial damage. Although it is not easy for the firm to deter all intrusion behaviors, the firm could learn from external information besides its own historical data in the current stage to adjust its best response to hackers in the following stage.

2.6. Conclusions

The ever-increasing global network continues to facilitate the collaborations within and among enterprises and also promote multinational corporations' expansion of market shares. In the meantime, it also increases the vulnerability of a firm facing the intrusion attacks around the world. In fact, the US-CERT, a part of the Department of Homeland Security, has reported more than 20,000 vulnerable, with the increasing rate of 50 to 60 per month, implying a world-wide

cost of more than $1 trillion dollars (US-CERT 2009). Various efforts have been undertaken by the research community in the last two decades to study detection of intrusions and increasing the precision of the detection mechanisms. Game theory, as one of the most commonly used approaches, offers many promising perspectives, insights, and models to address the ever changing security threats in cyberspace. However, almost all existing game theoretic methodologies concentrate on uniform hackers and defenders. They do not pay attention to the diversity in a hacker's intrusion behaviors, nor do they consider the firm's costs to investigate the abnormal activities. Our research is aimed at filling this gap and providing insights to explain the phenomenon of the increasing number of hackings, especially *international* cyberattacks.

Our game theoretical model captured the natural interplay between a firm's investigations and a hacker's intrusions as a "cat and mouse" game; most importantly, in our basic model, we demonstrated that *international* hacking cannot be fully prevented, no matter what strategy a firm adopts. In the extreme circumstance, no matter how severe the expected penalty, the firm will choose not to investigate if it believes there are too many *international* hackers. Fortunately, under a certain proportion of *international* hackers, the firm could prevent some *domestic* hackings, as long as the deterrents are large enough. This information provides some managerial insights for a firm to strategically allocate its resources to prevent inevitable intrusions and could improve the firm's profits, by treating security investments like costly insurance. Furthermore, our model of the continuous type of hacker provides the specific percentage of hackers who will be deterred by a certain level of heavy punishment.

Additionally, the fraction of damage recovered by the investigation process is another relevant factor. Moreover, by incorporating external signals (e.g., a newspaper report or other media channels) with the firm's historical data, we illustrate that equilibrium strategy profiles between a firm and hackers will switch from one to another, over time. Particularly, when a strong signal of *domestic* hackings is observed in a recent time period, the firm will be able to effectively stop some *domestic* hackers in the following stage with severe penalties. Our work also contributes to current IS literature by differentiating hacker types and considering the diversity in firm's investigation costs, as well as hackers' expected penalty. Moreover, we focus on the pure-strategy Bayesian Nash equilibriums, rather than mixed-strategy profiles, for the sake of more straightforward interpretations, which could better reconcile mathematical modelling with real life.

One of the future directions of this study is to allow the firm to have more than one type. And the firm's strategy action could be "investigate with pre-investments on security", "investigate without pre-investments", and "not investigate at all." Accordingly, we could characterize the level of investment firm should have for securing its information assets. Another research question could be the optimal update frequency of the firm's belief about hacker types based on its historical data as well as external signal effects. In our current study, we did not consider the discount factors with respect to the payoffs of the players. It will be interesting to incorporate decay factors (e.g., time cost for both players, hacker's benefit, etc.) into the model as the game is played by both players repeatedly over time.

CHAPTER 3. INFORMATION SECURITY POLICY COMPLIANCE: DESIGN AN INCENTIVE STRUCTURE TO PREVENT INSIDER DATA BREACHES

3.1. Introduction

In the age of information technology modern firms face vast challenges which could undermine their economic performance. For decades, information has been recognized as a valuable corporate asset, enabling an organization to add value to its products and services, reduce costs, and meet customer needs (van den Hoven 1999; Zhao 2004). Given the integral role of IT in today's enterprises, information security has to 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 ensure information security, organizations often rely on technology-based solutions (Ernst and Young 2008; PricewaterhouseCoopers 2008).

However, information security cannot be assured only by using technology solutions. Solid security products or technology alone cannot protect an organization without a good management policy and implementation. It is stated that information security is not primarily a technical problem but a management or business 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 in both technical solutions and employees' compliance with information security policies (Bulgurcu et al. 2010).

It has long been a well-recognized fact that companies' information security efforts are threatened by employee negligence and insider breaches (Loch et al. 1992), because employees are often the weakest link in information security (Mitnick and Simon 2001; Warkentin and Willison 2009). A survey conducted by the Computer Security Institute reported that the average monetary loss per respondent was $288,618, and that 44% of the respondents reported insider security-related abuse, making it the second-most frequently occurring computer security incident (Richardson and Director 2008).

To prevent the information security issues caused by internal personnel, 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 works take the more "gentle" approach, like rewards or incentives, to regulate their employees' noncompliance (Bulgurcu et al. 2010; Padayachee 2012; Pahnila et al. 2007; Vance and Siponen 2012). But, few papers incorporate both means to secure its information assurance (Chen et al. 2012; Liang et al. 2013). To the best of our knowledge, no extant MIS literature has done behavioral economics experiments to examine employees' compliance behaviors by truly engaging participants with paid benefits. A Sommestad et al. (2014) review paper has examined 29 studies with more than 60 variables related to information security policy compliance and noncompliance; however, no dominant variables were clearly identified due to their very small effect size. Most of those variables are measured through a self-report survey or a hypothetical single scenario-based experiment without permitting real incentives of participations; hence, we believe our study with multi-scenario-based measurements 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.

In addition, from a company's perspective, the distinct and extrinsic motivations of reward and punishment are two very practical ways for the company to discipline its workforce to minimize security breaches. A meta-analysis done by Balliet et al. (2011) revealed that both rewards and punishments exhibited a median to large effect on cooperation in general. In essence, security violation is different from regular policy misbehavior since a single data breach caused by a few employees may lead to the whole company suffering. Ideally, a company would like all its employees to cooperatively comply with the information security policy in order to prevent data breaches.

Although it seems to be rare to see a modern company employ a policy of collective rewards or collective punishment, it was commonly used in U.S. military boot camps in the 1980s (Gilham 1994). Heckathorn (1988) showed that when a group is subjected to collective sanctions (including collective rewards and collective punishment), it may encourage group members to monitor and regulate one another's behavior, although it may also infuriate group members to react against the agent that issues the threat, especially when collective punishment is imposed. If companies can balance well between reward and punishment, they could leverage the effect of collective sanctions to reduce employees' noncompliance. To the best of our knowledge, this paper is the first attempt to explore such collective rewards and collective punishments in the context of information security research.

Due to the small effect sizes of perceived sanction and perceived benefits by survey-type research, inconclusive effects of deterrence on information systems misuse, as well as concern for real companies' practice, our paper aims to assist companies to design a realistic and effective managerial policy and payment structure to prevent information security data breaches. Specifically, we would like to address the following research questions:

RQ1: How does monetary reward affect employees' compliance with an information security policy?

RQ2: How does monetary punishment affect employees' compliance with an information security policy?

RQ3: What is the combined effect of monetary rewards and punishments on employees' compliance with an information security policy?

RQ4: How do collective sanctions affect employees' compliance with an information security policy?

RQ5: How do monitoring systems affect employees' compliance with an information security policy?

The rest of the paper is organized as follows. The second section reviews the previous works in the information security literature in an organizational context. The third section develops our theoretical argument and core hypotheses. The fourth section discusses the research methodology and experimental design. The fifth section presents the data collection and analysis. The sixth section provides our experimental results with thorough discussions. The seventh section concludes our paper and elaborates its implication as well as limitations.

3.2. Review of the Literature

3.2.1. Human factors in information security and a firm's economics

The insider threat is always present and manifests itself in many ways in human society (Colwill 2009). There is a famous mythological story among Greeks, named the Trojan War. A huge wooden horse hidden with a select force of men inside was constructed and given to the city of Troy as a victory trophy. Under the ignorance and silence of insiders (i.e. the people of Troy), Greek forces crept out of the horse during the night and eventually defeated the Trojans. In modern organizations, despite the increasing enhanced information security systems of corporations, "Trojan-Horse" insiders (i.e. malicious employees) are emerging endlessly. In fact, the computer virus, Trojan horse, was developed through this concept. It infiltrated the backdoors of the "infected" computers and sent any wanted information back to the hackers. Spam email with the .exe attachment is one particular example of such a kind of attack. As soon as those noncompliant employees open (could be unintentionally, but still be noncompliant behavior) the .exe file, the company's information assets are compromised.

The security breach of Target in 2013 can very well illustrate 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 credential information were stolen through a phishing attack of malware delivered in an email at Fazio. Consequently, hackers used the stolen credential information from Fazio to remotely log into Target's inner network payment system,

stealing the payment and personal information of as many as 110 million customers, and then removed this sensitive information from Target's network to a server in Eastern Europe. This particular hack affected more than a third of the U.S. population, exposing 34% of American's financial information (Wallace 2014). This massive data breach directly led to a more than one percent loss of Target's stock price by the time of the report and a more than $148 million dollar loss to its shareholders (Abrams 2014). Furthermore, in order to maintain loyal customers, Target has been providing a free credit monitoring service for its customers, which further undermines its economic profitability. Additionally, the concern of information leaking prevents new customers from continuing to use Target's service, which indirectly hurts its corporate reputation. Moreover, Target has to constantly face an enormous number of lawsuits from its customers, which could further damage its goodwill.

Even in governmental organizations, insiders are prone to accidental 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 70% of fraud is perpetrated by insiders rather than by external hackers; however, 90% of security controls and monitoring of a company are focused on external threats (McCue 2008).

The cost of security breaches can be as much as $5.4 million in some organizations and each security attack can cause organizations an average cost of $591.780 (Alaskar et al. 2015). The Datalossdb Open Security Foundation website shows that about 24% of the total data-loss incidents in 2012 were due to insider employees, both by accident or maliciously. In addition, the ongoing PwC survey in the UK shows that 75% of information security breaches in large

organizations were caused by human factors in 2015. This figure is an increase from 58% one year ago (PwC 2015). Similarly, the Chronology of Data Breaches shows that approximately 9,232,015 records have been reported as insider data breaches in 2012 in the United States. The Ponemon Institute shows that 35% of data breaches globally were due to human errors (Alaskar et al. 2015).

Although external hackers are sophisticated, with advanced technology skills, numerous facts aforementioned and research papers (Bulgurcu et al. 2010; Herath and Rao 2009b; Hu et al. 2012; Hu et al. 2011; Myyry et al. 2009; Warkentin and Willison 2009) have shown that the human agent is still the weakest link in the defense against internal and external threats to organizational information assets. Nevertheless, no information security practice or technique is effective if not properly adopted by its users (i.e. employees) (Ernst and Young 2002; Puhakainen and Ahonen 2006). Therefore, making sure its employees comply with the information security policy and regulation is a great challenge for both profit and nonprofit organizations.

3.2.2. The principal-agent dilemma in the information security context

It is always hard to make people do things which are not convenient and easy, since it requires extra time and effort. In economic literature, such a phenomenon is theorized as the principal-agent dilemma or agency theory (Eisenhardt 1989). The principal-agent dilemma occurs when one entity (called the "agent") is able to make decisions on behalf of another entity (called the "principal") and the agent is motivated to act in his own interests, which are contrary to those of the principal. Specifically, the agents incur personal costs as they devote their time,

knowledge and effort to the principal; however the principal is not able to constantly monitor or assess the agents' efforts and thus the agents can retract the level of effort, skill, and knowledge they provide (Herath and Rao 2009a).

In order to motivate agents, the principal can either enhance the monitoring mechanism to identify "lazy" agents or develop an incentive structure to motivate the agents to work hard. In current industry practice, the incentive motivation or commission rewarding system is more commonly used, especially in the sale department of a company. A salesman's salary is usually composed as two parts, the base and the commission. The more items sold by him, the more commission he will earn. In this way, the incentive structure is designed to align the agent's interests with the principal's, creating win-win situations for both entities.

In an information security setting, it is rare to see a company reward those employees who are compliant with the information security policy. Instead, the more common practice identified by the literature is through the sanction. In organizational information security, the responsibility of whether to obey organizational security policies is delegated to employees (Herath and Rao 2009a). Employees may leak the company's information assets for their own benefits or simply ignore the security regulation for the sake of time. In fact, time saving has been identified as a major incentive to violate information security policies because employees perceive that security policies slow their work down with added procedures (Puhakainen and Ahonen 2006). As a result, employees' interest (the agents) is in conflict with the company's (the principal) as employees want more work done but the company wants more work done securely.

As said before, in order to solve this principal-agent dilemma, the company needs to "induce" employees to behave as it intends to by aligning both entities' interests. Similar to the salesman's example, the company could pay a bonus on top of the base salary to those employees who are compliant with the firm's information security policy. Essentially, the paid bonus could reconcile the conflict between employees' time saving with the company's security requirement as employees get extra pay for their "additional" time spent complying with the policy. However, both academic literature and industry practice seem not yet to realize this incentive structure in information security compliance as they currently rely on the perceived force of regulation policy (e.g. sanctions) and believe it is the employees' duties to obey the regulation and rules. As pointed out by current principal-agent dilemma literature review, information security policy compliance need not merely depend on the "stick", but the gentler way, the "carrot", is also effective and useful.

3.2.3. Employees cooperation for firm's information security

An information security policy violation is very different from a regular rule-breaking behavior, as the consequence of one instance can be amplified significantly. More often, one employee's noncompliance can result in a chain effect through the Internet systems and bring a huge disaster for the company, as illustrated by the previous Target 2013 example. A general would like all his soldiers to be equally strong, without having any vulnerability, to defeat the battle; similarly, the ideal situation for a company is that all its employees cooperatively fight for the "information battle" without any internal "capitulators". However, a "disobeying solider" is always hard to address. Nevertheless, how to increase cooperation in information security

compliance is rarely studied. In fact, to the best of our knowledge, the present research is the first attempt to address this issue.

"Good and evil, reward and punishment, are the only motives to a rational creature: these are the spur and reins whereby all mankind are set on work, and guided," said by John Locke in the late 1600's (Locke et al. 1989). He believed that incentives, both rewards and punishments, are effective tools to regulate individuals in their pursuit of self-interest. In fact, the biological and social sciences research has shown that incentives provide a powerful solution to increase cooperation (Edney and Harper 1978; Fehr and Gächter 1999; Hashim and Bockstedt 2015; Henrich 2006; Lynn and Oldenquist 1986; Ostrom et al. 1992; Rand et al. 2009; Sigmund 2007; Yamagishi 1986). As the company wants its employees to cooperatively comply with its information security policy, providing incentives for cooperation will encourage each individual employee to sacrifice her/his self-interest for the collective benefit of the company.

In an organizational information security setting, the positive incentives (reward) for those employees who comply with the policy will establish positive reinforcement links among all employees in that group to achieve the rewards together; similarly, the negative incentives (punishment) for those noncompliant employees will cause negative reinforcement links among them in the same group to avoid the punishment cooperatively. In the extreme, the punishment of those compliant employees due to the noncompliant ones will further the "cooperation" between employees since each individual will face the condemnation and judgement from others; it essentially increases the mutual surveillance among employees. On the other hand, the given reward can only be earned when all employees behave (i.e., obey rules) cooperatively. Everyone

wants to get the reward and thus becomes spontaneously self-disciplined. This collective reward and punishment is formally described as a collective sanction (Heckathorn 1988) and will be discussed in greater detail later.

The information security capability of a firm is not merely dependent on its hardware-software sophistication, nor on some employees' good compliance, but on the cooperation in compliance among all its employees to secure the information assets. As the commonly-known barrel effect manifests, the capability of a firm to secure its data asset against its insider breach is heavily dependent on those few noncompliant employees rather than the majority who are compliant. Therefore, information security compliance is not simply an individual matter, but requires employees' cooperation to attain.

3.3. Theoretical Argument and Core Hypotheses

According to Alaskar et al. (2015)'s review paper, the General Deterrence Theory is still the dominant theory used by IS scholars to study information security (Chen et al. 2012; Cheng et al. 2013; D'Arcy et al. 2009; D'Arcy and Hovav 2009; Guo and Yuan 2012; Harrington 1996; Herath and Rao 2009a; Herath and Rao 2009b; Lee et al. 2004; Siponen and Vance 2010; Son 2011; Straub Jr 1990). Straub Jr and Nance (1990) adopted the classical deterrence theory from criminology literature into their information security studies. The deterrence theory asserts that individuals weigh costs and benefits when deciding whether or not to engage in criminal behavior (Siponen and Vance 2010).

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 (Sommestad et al. 2014) found out that general deterrence theory has questionable efficacy since its effect size, β-value, is on average lower than 0.10. In spite of the survey methods used, which have self-reported bias, measuring intention as the dependent variable in those papers, the small effect size of the perceived severity of sanction and the perceived certainty of sanction have limited explanation power over employees' noncompliance behavior. Hence, deterrence alone will not eliminate information breaches.

3.3.1. Rational choice theory

Rational choice theory can be seen as a modern extension of classical deterrence theory, which originated during the late 18th century with the work of Cesare Beccaria, and is a prominent theory in Criminology (Cao 2004). Becker (1974)'s Economic Theory of Crimes indicates that criminal behavior is rational and goal-oriented based on the offender's assessment of perceived costs and benefits. Rational choice theory explains individuals' decisions to commit crimes as utilitarian calculations based on their rational choices weighing means and ends (Cornish and Clarke 1987). Although the theory is commonly used to explain criminal behavior, it is also capable of being generalized to cover all violations (Becker 1968), and is thus applicable to the study of violations of organizational IS security policies.

In our information security research setting, we follow the typical economic assumption that people are rational, which means employees are selfish, seeking benefit and avoiding punishment. In addition, we also assume that the company has full knowledge (i.e., complete

information) about each employee's behavior. In other words, we assume the company has perfect monitoring/surveilling systems to detect each employee's action when they are facing information security temptations (this assumption will be relaxed later). Accordingly, based on the rational choice theory, we expect the following hypotheses,

H1: Reward for compliance will have a positive impact on employees' behavior in complying with a company's information security policy.

H2: Punishment for noncompliance will have a positive impact on employees' behavior in complying with a company's information security policy.

Furthermore, rational choice theory also indicates that the effects of reward and punishment are not contrary to one another, but complementary to each other. At least, reward and punishment together should have an additive effect not a cancelation effect. As an individual is a rational thinker and weighs the costs and benefits, she/he may simultaneously assess the reward gained by compliance and punishment received by noncompliance. Accordingly, the optimal choice for her/him is to choose to comply since she/he can get rewards and avoid punishment. In fact, almost all extant MIS literature treats reward and punishment separately, ignoring the complementary relationship between two treatments. The current literature heavily focuses on surveying participants for their compliance intentions and isolating perceived reward and perceived sanction.

In contrast, we expect a company should have a better outcome by providing both positive and negative incentives for compliant and noncompliant behaviors of its employees. Accordingly, we expect the complementary effect between reward and punishment will outperform either single treatment,

H3: Reward for compliance and punishment for noncompliance together will have stronger impact on employees' behavior in complying with a company's information security policy when compared with either a reward only or a punishment only mechanism.

3.3.2. Collective sanction

Collective sanction is the system where rewards or punishments extend not only to the actor but to the actors' group (Heckathorn 1990). In such systems, when an individual violates or complies with a rule, not merely the individual but other members of that person's group as well, are collectively punished or rewarded by an external agent (Heckathorn 1988). When properly used, collective sanction could enhance mutual surveillance to reduce noncompliant behavior and hence create norms and culture to enforce wanted behavior. The literature on principal-agent and cooperation in compliance shows that reward and punishment are two distinct and effective means to enhance compliance with an information security policy. However, as said before, the level of a company's information security defense is determined by the few noncompliant employees rather than the compliant majority. Hence, the ultimate goal for a firm is to enhance employees' cooperation in compliance.

In a modern firm, it seems that collective sanction is rarely used in practice. But, it is commonly used in U.S. military boot camps to enhance the effectiveness of control for cooperation (Gilham 1994). A more extreme application of collective sanction occurred in Stalinist prisons (Dallin and Nicolaevsky 1947), where prisoners earned points through work and compliance with prison rules and the distributions of food, medicine, and other essentials of life depended on the points earned by the group. Although the use of collective sanction may sound cruel, the company may well leverage its benefit when adopting it properly. Combined with the solution of the principal-agent dilemma, the company could reward all or punish all by giving additional incentives or taking away the extra incentives without changing base salaries. This principle of payment structure may be more effective than the traditional deterrence mechanism.

In the cooperation literature, incentives have been seen as the structural solutions to resolving social dilemmas by reducing conflicts of interest (Kollock 1998; Van Lange and Joireman 2008; Yamagishi 1986; Yamagishi 1988). The meta-analysis paper by Balliet et al. (2011) provides unequivocal evidence that rewards and punishment are effective factors for cooperation in social dilemmas, explaining about 3% to 12% of the variance in cooperation. Furthermore, it also shows that people are more willing to cooperate when the collective incentive is given and the self-interest incentive is reduced. Therefore, employees may be more regulated when the firm imposes collective punishment to punish all due to the noncompliance of some employees. Meanwhile, employees may be more motivated when the firm grants collective rewards to reward all as long as no noncompliant behavior occurs.

However, collective sanction can also have exactly the opposite effect, as Heckathorn (1988) points out that a group threatened by collective punishment could react by attacking the agent and hence motivate group rebellions. Furthermore, when attacking the external agent is not available and group members are not able to identify each other, collective sanction could lead to heterogeneous non-cooperation and convergence to a decreasing equilibrium in cooperation over time. Fehr and Gächter (2000) conducted an experiment based on the repeated Public Goods game and they found that the level of cooperation is declining when group members are not allowed to punish non-cooperative members. Andreoni et al. (2003) used a one-shot anonymous Proposer-Responder game to illustrate that people are willing to sacrifice personal interests to punish those non-cooperative ones and reward those cooperative ones to achieve high cooperation. Gürerk et al. (2006) did another study, also based on the repeated Public Goods game, to show that the sanctioning institution (allowing anonymous group members to punish others for noncooperation) maintains a higher level of cooperation compared to a sanction-free institution. The more recent paper by Rand et al. (2009) indicated that it is not the punishment per se that sustains the high cooperation in the repeated Public Goods game, but rather the possibility of targeted interactions between group members.

In the setting of the Public Goods game, the low level of cooperation is reflected by the individual group member's small amount of contributions to the "common goods". Accordingly, it would lead to the benefit of entire group suffering, especially for those group members who contribute a lot but receive so little. Hence, such indirect collective sanction may actually undermine the cooperation even in information security compliance. In fact, Heckathorn (1988, p. 556) said, "collective sanctions create ambivalent incentives" for compliance in a group.

Therefore*, it seems ambiguous how collective sanction may affect employees' behavior in complying with a company's information security policy compared with individual incentives, especially when employees are unable to identify others' compliant or noncompliant behaviors.* Instead of proposing hypotheses for collective sanction, we will explore its impact on cooperation in security compliance and discuss its theoretical boundary conditions.

3.3.3. Complete and incomplete information about monitoring

Previously, we assumed the company had complete information about employees' behavior in information security policy compliance. More realistically, a company usually relies on some sort of detecting systems (e.g., Intrusion Detection Systems) for monitoring the input/output information traffic for alerting abnormal activities. Khan et al. (2007) shows that the detection accuracy rate could range from 11% to 95% in their static benchmark data set. However, such detecting systems are never perfect in the real-world setting. In fact, numerous research done by computer science and computer engineer scientists (Anderson et al. 1995; Garcia-Teodoro et al. 2009; Ilgun et al. 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 et al. 2003) still cannot show a definitive accurate rate of the IDS detection. This is because the IDS constantly generates an unknown number of false positive and false negative alarms, which is directly caused by the dynamic nature of an unknown number of genuine attacks, especially when the vulnerabilities are newly discovered. Nevertheless, the agency theory acknowledges the incomplete information gained by the principal and hence it gives the agent opportunity to retract the level of his effort. Therefore, in the context of information security policy compliance, we would expect that the low chance of being caught would undermine the effect of

reward and punishment on employees' compliance with information security policy. Boss et al. (2009)'s paper further proves that if one knows he/she is been watched, he/she will follow the information security policy; otherwise, the requirement will be often ignored due to the additional costs of time and effort required to comply with the security policies and procedures. Accordingly, we compose the following hypotheses,

H4: A low chance of being caught will have a negative impact on employees' behavior of complying with a company's information security policy.

H5: A low chance of being caught will reduce the positive effect of Reward for promoting employees' behavior in complying with a company's information security policy.

H6: A low chance of being caught will reduce the positive effect of Punishment for preventing employees' behavior in noncomplying with a company's information security policy.

3.4. Research Methodology and Experimental Design

3.4.1. Scenario-based security compliance measurement

Both review papers by Sommestad et al. (2014) and Alaskar et al. (2015) clearly point out that the survey is the predominant research method used in information security literature. It is well known that using self-reported data is biased, especially in studying anti-social and ethical/unethical behavior (Krumpal 2013). Instead, scenario-based methods are more suitable to overcome such challenges by providing hypothetical situations (Pogarsky 2004). In the field of

IS, the 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 moral reasoning on employees' compliance with information security policies. Cheng et al. (2013) also use a single scenario test and develop an integrated model based on social control and deterrence theory to study information security policy violations. D'Arcy et al. (2009), Barlow et al. (2013), and Hu et al. (2015) use multiple scenarios to measure the employees' information compliance/noncompliance, whereas, other papers randomly assign one scenario per participant (Chen et al. 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 are not asked to respond directly in the first- or second-person manner. Due to the secrecy involved in the undesirable behavior, individuals are more likely to conceal their real response to the questions and provide the socially desirable answers to the researcher (Trevino 1992). However, the hypothetical scenario could make participants feel less afraid 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); whereas, plain survey questions usually ask participants in general terms.

In our research setting, we adopt the multiple scenarios of those minor and major violations developed by Hu et al. (2015). In total, we use 30 scenarios for measuring each

participant's behavior in complying with an information security policy. It not only methodologically reduces our measurement error, but also increases the generalizability of conclusions, as the large number of scenarios is more likely to capture more realistic situations in real practice. In general, all participants across Experiment 1-4 will be instructed to imagine herself/himself as a hypothetical employee called "Josh" of a "company". She/he will answer the given 30 scenarios on behalf of Josh. We only adopted those 15 minor and 15 major hypothetical security policies and ignored their control scenarios. Specifically, we will present participants in a pseudorandom order (the order of the stimuli scenario is randomized but consistent across all participants) omitting Hu et al. (2015)'s control group ones. By doing so, it will help to prevent those unknown effects which may be caused by the different order of scenarios across different participants.

3.4.2. Real dollar treatment vs. perceived treatment

Although our literature review indicates that hypothetical scenario-based methods are widely used in the IS field for studying information security research, the technique used in the scenario-based experiments which involve paying for study performance is rarely seen in the IS literature. Instead, this paper adopts the behavioral economics approach to pay participants for their completion of study tasks. By doing so, we can truly engage participants with the study design as their earnings are dependent on their task performance. This is a significant methodological contribution to the IS literature, as a great deal of experimental economics literature has shown that real dollars make a difference.

In the group level for cooperation, Balliet et al. (2011)'s meta-analysis shows that both rewards and punishments are more effective when participants are actually paid for their decisions rather than when making hypothetical decisions without monetary consequence. Furthermore, incentives seem to matter more when the monetary stakes are greater. For the employee-information-security compliance dilemma, the very practical action for a company is to design a suitable and effective incentive structure to motivate employees to align their self-interest with the company's benefit. Balliet et al. (2011)'s paper further points out that incentives are more effective in monetary forms or when incentives are framed according to the pecuniary benefits of cooperation. Thus, the behavioral economics approach with heterogeneous cash payment involved in the study will further our understanding about how reward and punishment influences employees' behavior of cooperatively complying with an information security policy.

3.4.3. Experimental design

There are four experiments in our study. Experiment 1 is a basic 2x2 factorial experimental design containing four groups of subjects. It evaluates the effect of individual reward and individual punishment. In addition, we test if individual reward and individual punishment together are not simply adding to one another, but rather have a super-additive effect. Experiment 2, with three groups of participants, introduces collective sanctions (including collective reward and collective punishment) to compare its result with Experiment 1's. We explore how exactly collective sanctions influence employees' compliance and hope to resolve its ambivalent effect of cooperatively compliance. Experiment 3, building upon Experiment 1, uses the 2 x 2 factorial design incorporating the concept of the company's degree

of monitoring. It is more realistic for a company to install an automated detection system (e.g., IDS) to inspect its employees' noncompliance rather than monitoring everyone, if possible. We consider how the monitoring affects individual incentives (individual reward, individual punishment, and individual reward and punishment) on employees' compliance. Lastly, Experiment 4, with three groups of subjects, is the most comprehensive design, including both collective sanctions as well as monitoring. This experiment permits us to give a company the most practical and realistic recommendations for regulating its employees' information security policy violations. It is worth noting that Experiment 1 uses individual-based interventions, whereas, Experiments 2-4 are group-based interventions. Each group is randomly composed of 5 participants and the group members are fixed without reshuffling through the entire experimental session.

Each participant was given 500 endowment tokens (100 tokens = $1.3) to use in this study. If a subject chose "Yes" after any given scenario, they had a chance to gain some self-benefits from 0 to 30 tokens depending on the severity of the specific scenarios. Subjects were told that the more severe the security breach of the scenario, the more tokens they earned. However, the real integer tokens associated with a certain scenario were randomly selected from a uniform distribution from 1-9 for minor and 11-30 for major violations. Hu et al (2015) classified each of the 30 scenarios as major or minor. In addition, we used 10 tokens as either reward or punishment. We believe using 10 as the separation point with randomization could well capture the fuzzy utilitarian calculations in an employee's mind when facing security temptations. It is worth noting that the specific tokens associated with a certain scenario is unknown to lab participants to avoid their calculating the costs and benefits of a particular

decision. Because we believe this design mimics the real-life situation as a noncompliant employee generally would not know the concrete amount of gained benefits before committing the violation behavior, but rather would have a rough idea based on violation severity to assess if it is worth doing. The specific order and token worth of each scenario is attached in appendix A. The instructions for participations of each group of four experiments are also attached as Appendix B. It is worth noting that we kept the instructions as neutral as possible by referring to the punishments and rewards simply as changes to participants' payoff.

Two main treatments in this experimental study were Reward and Punishment, which were reflected by tokens taken from or given to participants. If they chose "Yes", they lost 10 tokens as punishment; however, if they chose "No", they earned 10 tokens as reward. Meanwhile, whenever they chose "Yes" across all four experiments, the aforementioned self-benefit tokens were always applied to them. In addition, we conducted all four experiments through the oTree environment, an open-source Python and Django based platform for laboratory, online and field experiments (Chen et al. 2016). The following Table 1 is an overview of our four experiments with their respective 14 treatment groups (please see Appendix C for the specific designs of our four sequential experiments).

Table 1 Experimental Design Overview

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

3.5. Data Collection and Analysis

3.5.1. Participants

Student participant data was collected and used in our study. We examine participants' behaviors from a very broad sense, meaning we treat employees homogeneously although we do control for their risk tendency, impulsivity, age, gender, education, etc. For those employees who have hatred towards to the company, or have psychological problems are not the focus of current study. In other words, our study focuses on how extrinsic motivations will help a company to regulate employees' non-compliant behavior.

Although we acknowledge that using student subjects is a convenient sample, Siponen and Vance (2010) and Vance and Siponen (2012) have shown that work experience is irrelevant to participants' behavior of complying with information security policies, which is consistent with our results that students' organizational experience is not a significant factor for information security policy violation. In addition, we argue that using student subjects is appropriate for our research questions, for the following three reasons. First, we do not study the intrinsic motivation, like commitment to a company. Instead, we study the fundamental materialism-view extrinsic motivation of an employee, which assumes an individual is selfish and incentive driven (seeking for benefit and avoiding punishment). This principle will apply to most populations, including student subjects. Therefore, student subjects could be a good proxy for employees. Second, students are the future employees no matter whether they will stay in industry or academy. Security research has a common drawback. We study those phenomena that have occurred rather than develop a mechanism to prevent further incidences. If the proposed incentive structure works for current students, it will have a good chance of working well for future employees as well. Finally, students are similar to those young employees who are sometimes unwilling to follow rules due to their energetic minds. Hence, if we can make students comply and build a good culture/mechanism to sustain compliance, we have a good chance that the formal and senior employees will comply with the policy as well based on the institutional effect.

3.5.2. Data collection

Lab experimental data was collected at a large mid-west public university and, to enhance the generalizability, from two populations of English speakers within that university. The first

population comes from the business-major students' subject pool, which has about 900 students. This is the same subject pool used by Hu et al. (2015). The students are completely different, which ensures no participants can have seen our research scenarios before. Students signed up for the research study voluntarily. For those students who showed up in the study location, they received course credit and $10 on average to complete the study. Their final compensation depended on their task performance, which is incorporated in experimental treatments and was introduced in the aforementioned Experimental Design section. In total, 285 students participated in our experiment.

The second population is general undergraduate students, excluding the previous population, which is about 24,000. The principal investigator sent out invitation emails to the general students on campus. The email list of students was purchased from the university's Office of the Registrar. About 400 emails per wave with 59 waves of recruiting emails were sent out for the study. The recruitment email included information such as time length of the study, study location, compensation and eligibility of the study. In addition, students were given a Doodle Poll link to fill out their email address and choose suitable time slots to participate if they were interested in the study. There were about 600 students who signed up the study and 360 students who showed up in the study location. Those students who showed up received an extra $5 for their participation instead of course credit reward. All other incentive and experimental treatments remained the same as for the first population. No students from both populations were permitted to participate in more than one experimental section.

3.5.3. Experimental procedure

The data collection from the first population was conducted from the end of September to the mid-October, 2016. Meanwhile, general students' data from the second population was collected from late October to mid-November. Each experiment section lasted about 45 minutes. The principal investigator kept the time of experiment sections same regardless student populations. Experiments were conducted on every Tuesday, Wednesday, and Thursday from 3:00PM to 4:00PM, 4:00PM to 5:00PM, and 5:00PM to 6:00PM. Experimental procedures for the two populations are illustrated in the following.

For business students, they were recruited by the specialized time management online platform provided by the subject pool administrator. Students can log into the web-based software by their own credentials to choose available time slots. Meanwhile, an email reminder was sent out each week to remind students to participate in our study. One day before the experiment time slots, the principal investigator sent out another reminder to those signed students to confirm the study location, study time and other requirement like bring a pen or pencil.

After students arrived at the computer lab, they were greeted and instructed to sit at least one empty seat between each other to prevent collusion. Students were informed that personal devices, internet surfing, watching YouTube, etc. were not permitted. Then, the principal investigator used a script to introduce the overview of the experiment to students to enhance their comprehension. After consent forms were distributed, students were given whatever time they needed to read it through and sign the form. Then, they went through the first part of the

experiment, which is the 30 scenario-based questionnaires. To enhance the treatment manipulation, the core instruction was repeatedly displayed underneath each scenario when participants were making their decisions. For the specific intervention of each experimental groups, please see the Appendix B. Although a timer was embedded into the online user interface for each scenario to enhance the manipulation of treatment and control students' reading speed, those who finished earlier than others were instructed to wait patiently. After students made their decision for each scenario, a current summary of tokens earned was displayed. At the end, after all 30 scenarios finished, students were informed how much cash they would receive from the study. Then, after all students finished the first part of the study, they were given the password to access the second part of the study, which is a Qualtrics-powered 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 in order to get paid. Then, they were instructed to log off their computers to ensure their privacy and to receive their payment (concealed in an individual envelop) from the principal investigator. After students received their payments, the experiment session ended. Meanwhile, the principal investigator granted the course credit to students via the aforementioned online time management software.

For general students from the campus, they were recruited by email invitations sent directly from the principal investigator. A Doodle poll anonymous link was included for each invitation email. Students who were interested in our study could follow the link to choose their

desired time slots. It is worthy of mention that the Doodle poll is pre-configured to hide participations' emails and names from the public to preserve their privacy. Only the principal investigator and those faculties who have IRB clearance of the project are permitted to see participations' information. The same as business student population, one day before the experiment section, the principal investigator sent out the confirmation/reminder email to students to inform them the study location, study time and other requirements, like bringing a pen or pencil. The experimental procedures for general students were the same as the business students except for an additional step. After students finished reading and signed the consent forms, they were immediately given a $5 show-up fee to thank them for their participation. Meanwhile, they signed a payment receipt form required by the university controllers. After each experimental session finished, no course credit was given to general campus students.

3.5.4. Data-analysis procedure

Each scenario question was only given two choices, "Yes" or "No", for each participant to choose on behalf of the hypothetical third-person, "Josh". "Yes" means non-compliance, whereas "No" means compliance with the information security policy. The unit of analysis for our treatment effect is each treatment group, as our research focuses on how to design an incentive structure to intensify employees' cooperative compliance. In addition, to further control the potential effect caused by the different wording of 30 scenarios, we conducted the treatment-effect data analysis in the following procedure. First, we calculated the scenario-based Compliance Ratio for 14 treatment groups. The Compliance Ratio for each scenario in a certain treatment group is the proportion that the number of participants who chosen "No" divided by the total number of participants in that treatment group. For instance, the Compliance Ratio for

Scenario 1 in the Control group of Experiment 1 (Exp1C) is 0.714286, since 35 out of 49 subjects chose "No" in this treatment group. Second, we calculated the pair-wise Difference of Compliance Ratio (DCR) between 14 treatment groups, which yielded to 91 series of numbers of 30 fractions. This was done to control the potential effect of 30 different 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. This is the individual Reward treatment effect (without the confounding caused by scenario wording) compared with the basic control group. Third, we conducted a time series data analysis to test if the 91-respective means of 91 series of DCR numbers are not equal to zero. Particularly, we used an autoregressive model[1] with AR=1 because we suspect that each treatment group's current decision may be correlated to its previous one decision through the 30-repeated observations (i.e., 30 scenario questions), as we showed each subject the scenario questions one by one on the screen of the lab computers. Lastly, we obtained the t ratio and p value of the constant term in the time series data analysis to conclude if the respective treatment has effect or not.

In addition, we wondered if participants' demographic and other control variables would have impacts on their decision making for choosing "No". Hence, we also conducted a Logistic Regression with dummy codes for controlling scenario difference, but we had to switch the unit of analysis from treatment group level to each participant level in order to test those additional variables.

[1] 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 91- series of DCR to obtain the best fitting models by AIC index. For the sake of model concise and parsimonious, we adapted AR=1 autoregressive model 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.

3.6. Experimental Results and Discussions

Our overall experimental results can be best summarized in the following Table 2. It shows the coefficient and p-value of the constant term of the autoregressive model for all 91 DCR combinations. The shadow areas present those p-values which are less than 0.05.

The complete output of AR=1 model is attached in Appendix E. In our time series data analysis, the constant term represents the expected difference of two means between their respective treatment group. For example, the expected difference between Exp3C and Exp1C is -0.038 with a p-value as 0.015, which indicates the low chance of being caught has a significant negative impact on information security compliance compared with the most basic control group.

Table 2 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

3.6.1. Experiment 1 and discussions

Based on the Rational Choice Theory, we designed the Experiment 1 to discuss how individual reward and punishment influence employees' compliance. The expected difference of Exp1P – Exp1C is 0.026 with a p-value as 0.210, which shows that individual punishment has no significant impact compared with the control group. In other words, imposing individual punishment to noncompliant behavior does not statistically improve employees' compliance with

information security policy. Hence, our hypothesis 2 is not supported. Although it is not supported, it may well illustrate why current popular strategy (deterrence only mechanism) cannot effectively prevent insider data breaches.

However, the expected difference of Exp1R – Exp1C is 0.101 and extremely significant with a p-value less than 0.001. This indicates that individual reward works very well for regulating employees' noncompliant behavior. Therefore, hypothesis 1 is supported. In addition, when we compare Exp1RP and Exp1C, a positive difference in means (0.193) and extremely small p-value (< 0.001) is found. Furthermore, the expected difference of Exp1RP – Exp1P is 0.167 (p-value < 0.001) and Exp1RP – Exp1R is 0.093 (p-value < 0.001). This illustrates that individual reward and punishment together is significantly better than either individual reward or individual punishment. Thus, our hypothesis 3 is strongly supported. This finding is consistent with Andreoni et al. (2003, p. 901) saying "the absence of a reward is not equivalent to a punishment", as rewards and punishments are complementary to each other.

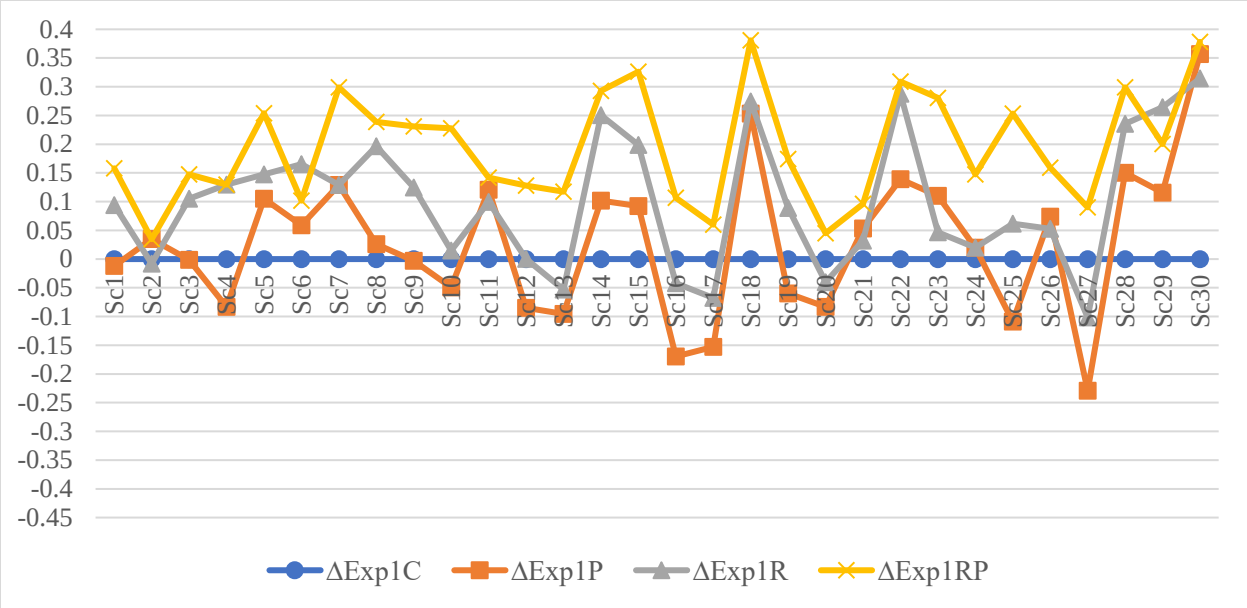

Figure 1 Exp1: Individual Reward and Punishment

The above Figure 1 shows the Difference of Compliance Ratio for all 30 scenarios in Experiment 1 when Exp1C is used as the subtracted base. Figure 1 further evidences that individual reward and punishment together has better regulation power over either individual reward or individual punishment. In fact, when reward and punishment is used together, it can help to sustain the high compliance rate compared with either individual treatment. The effect of reward and punishment is complementary and enhanced when both methods are presented simultaneously because it can constantly deviate employees from their self-interests and motivate them to continuously comply with the information security policy. Additionally, Andreoni et al. (2003) pointed out that it may be a mistake when only rewards, omitting an option for punishment, is used to design an institution. Based on our results, we believe designing an incentive mechanism around punishment only and omitting reward may also be a mistake, although such strategy is commonly used in current practice of protecting information security.

Furthermore, we also compared reward and punishment in complying with information security policy. We found that the expected difference of Exp1R – Exp1P is positively significant with a p-value less than 0.001. It means reward is more powerful than punishment for preventing insider data breaches caused by employees. This is an interesting result, although the extant majority literature found that perceived punishment is more effective than perceived reward (Bulgurcu et al. 2009; Bulgurcu et al. 2010; Liang et al. 2013; Pahnila et al. 2007; Siponen et al. 2010; Vance et al. 2012). This literature all used survey as measurement mean, which did not allow differentiated incentives to engage survey takers. Such method suffers from self-report bias as survey takers tend to provide socially desirable answer to the questionnaires (Krumpal 2013). In addition, the survey method tends to ask participants about information security compliance in a general fashion, which is almost impossible to capture one's genuine thought when facing temptations. Instead, our behavioral economics approach with hypothetical multi-scenario based measurement further revealed the superior regulating power of reward compared with punishment in an information security policy compliance setting.

Although violating information security policy is socially undesirable/unethical behavior or may even be illegal behavior, a company frequently delegates the compliant responsibility to employees' ethics or moral standards (Herath and Rao 2009a). 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 and Ahonen (2006) showed that employees perceive that the security policy slows down their work with added procedures. As discussed

earlier in the literature review section, providing rewards for employees to put effort into complying with the security policy will reconcile their unwillingness for additional time spent in security procedure, although such compliant behavior ought to be their obligations. After all, a company paying a little extra reward to prevent huge data breaches is more beneficial and less disruptive.

3.6.2. Experiment 2 and discussions

Our Experiment 2 was particularly designed for studying how Collective Sanctions (Collective Reward and Collective Punishment) influence employees' compliant behavior. Based on Table 2's statistical results, it seems that in general Collective Sanctions have negative impacts on employees' compliance. The expected difference of Exp2P – Exp1C is -0.091 with a p-value less than 0.001 and the expected 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 reward or collective punishment. This might be the reason why it is very rare to see an American company either reward all their employees, when they all cooperatively complying, or punish all including complaint employees, when someone is breaking the security policy.

Furthermore, the impact of collective sanctions on employees' cooperation in security compliance can be explored by comparing individual reward with collective reward and individual punishment with collective punishment. Specifically, the expected difference of Exp2P – Exp1P is -0.118 with a p-value less than 0.001 and the expected difference of Exp2R – Exp1R is -0.252 with a p-value is less than 0.001. The expected difference of Exp2RP –

Exp1RP is -0.180 with a p-value is less than 0.001. All these results show that collective sanctions undermine the individual sanctions (i.e., individual reward or/and individual punishment) in our research setting. Remember, our theoretical augment mentioned that collective sanction could promote as well as undermine cooperation in compliance. The following figure will provide more behind-the-scene details.

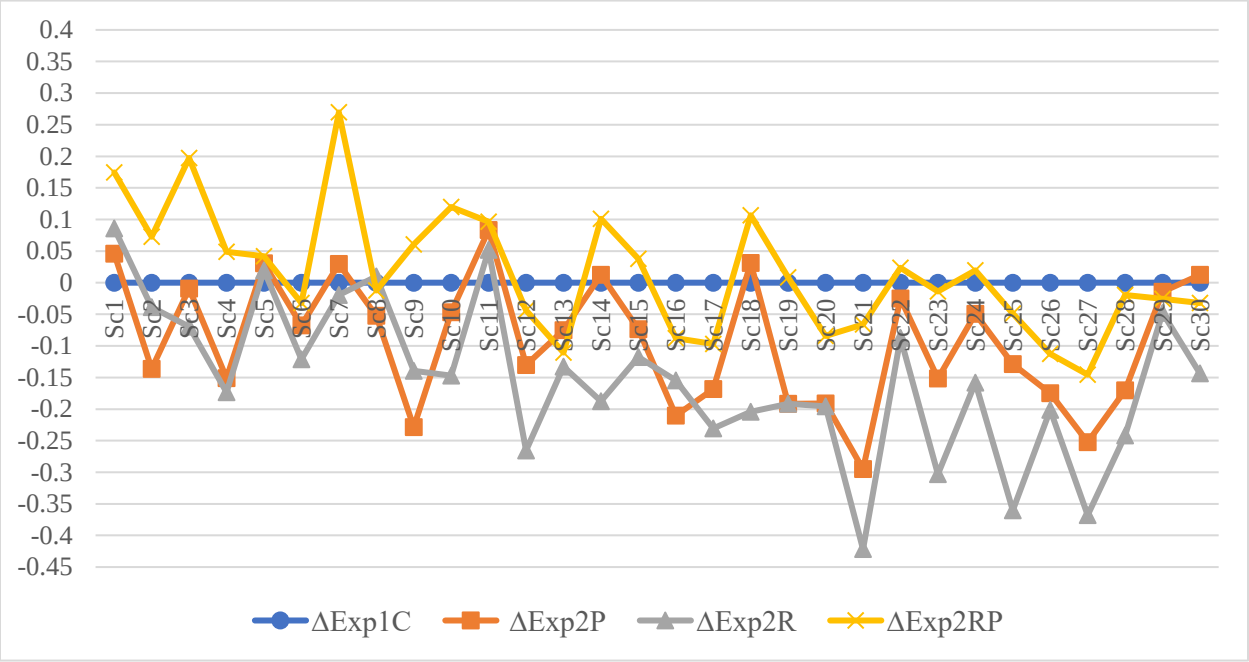

Figure 2 Exp2: Collective Reward and Punishment

Figure 2 presents the Difference of Compliance Ratio for all 30 scenarios in Experiment 2 when Exp1C is used as the subtracted base to control the scenarios' difference. Clearly, it shows that collective sanctions have a spiral-downward impact on cooperative compliance with information security policy. This declining trend is consistent with Fehr and Gächter (2000)'s stranger-group experiment without punishment option, although there is a distinct difference between our work and theirs. They studied how giving group members the option to punish non-

cooperative ones to enhance overall contribution in a Public Good game. Our collective punishment, as defined by Heckathorn (1988), is more similar with their no-punishment-option group with an external punishing force. In other words, we study how external punishment will impact on group members' cooperation in compliance.

Initially, collective sanctions seem to have stronger regulating power over individual sanctions (compared with Figure 1) in Scenario 1, especially for the collective punishment. However, it cannot sustain even though both reward and punishment mechanism is presented (illustrated by ΔExp2RP). Then, the regulating power starts to weaken and converge to an inferior equilibrium when more and more people commit noncompliant behavior. This could be explained by the following. Fehr and Fischbacher (2003) found that a minority of altruists can force a majority of selfish individuals to cooperate when cooperators are given the opportunity to punish directly to defectors. Meanwhile, Rand et al. (2009) showed that it is not the punishment option but the targeted interaction for sustaining cooperation in contributing the public goods game. Therefore, we argue that when the compliant majority (initially) are not given the option to target those minority of noncompliant ones, a few noncompliant behaviors (under the environment of collective reward or/and punishment) will stimulate reciprocal selfishness and bitterness due to tit for tat among group members to seek their own self-benefit, which will gradually collapse the cooperation in security compliance.

Although both collective reward and collective punishment have declining regulating power, collective reward tends to diminish more rapidly than collective punishment for security compliance. In fact, the expected difference of Exp2R – Exp2P is -0.060 with a p-value less than

0.001. This indicates that collective punishment is more effective than collective reward, although our Experiment 1 shows individual reward is more powerful than individual punishment. Remember, the collective reward will be given to all employees when no one is breaking the policy. Instead, the collective punishment will be imposed on all employees as long as someone is violating the rules. Generally, the possibility for all group members to comply is much less than for someone in the group to not comply with the security policy. Therefore, such small-chance condition significantly undermines the superior regulating power of collective reward compared with collective punishment, which implies that collective reward should not be used in a large group-size setting.

Lastly, the expected difference of Exp2RP – Exp2P is 0.106 with a p-value less than 0.001 and the expected difference of Exp2RP – Exp2R is 0.168 with a p-value less than 0.001. This means that collective reward and punishment together outperform either collective reward or collective punishment, which is consistent with our result in Experiment 1. In addition, Figure 2 also demonstrates the similar patterns as Figure 1 for this finding. This further demonstrates that reward and punishment are complementary to one another no matter whether they are in individual forms or collective forms.

3.6.3. Experiment 3 and discussions

So far, we have studied how rewards and punishments affect employees' security compliance in a perfect detection environment. However, as pointed out earlier, such detection system cannot be faultless in the real world. Hence, our Experiment 3 was conducted to understand how a low chance of being caught influences employees' compliance behavior. The

expected difference of Exp3C – Exp1C is -0.038 with a significant p-value of 0.015. Hence, our hypothesis 4 is strongly supported, as a low chance of being caught has a negative impact on employees' behavior of complying with a company's information security policy. Furthermore, the expected difference of Exp3P – Exp1P is -0.117 with a p-value less than 0.001, the expected difference of Exp3R – Exp1R is -0.069 with a p-value of 0.043, and the expected difference of Exp3RP – Exp1RP is -0.175 with a p-value less than 0.001. These results strongly support our hypotheses 5 and 6 that the low chance of being caught undermines the regulating power of individual reward or/and individual punishment.

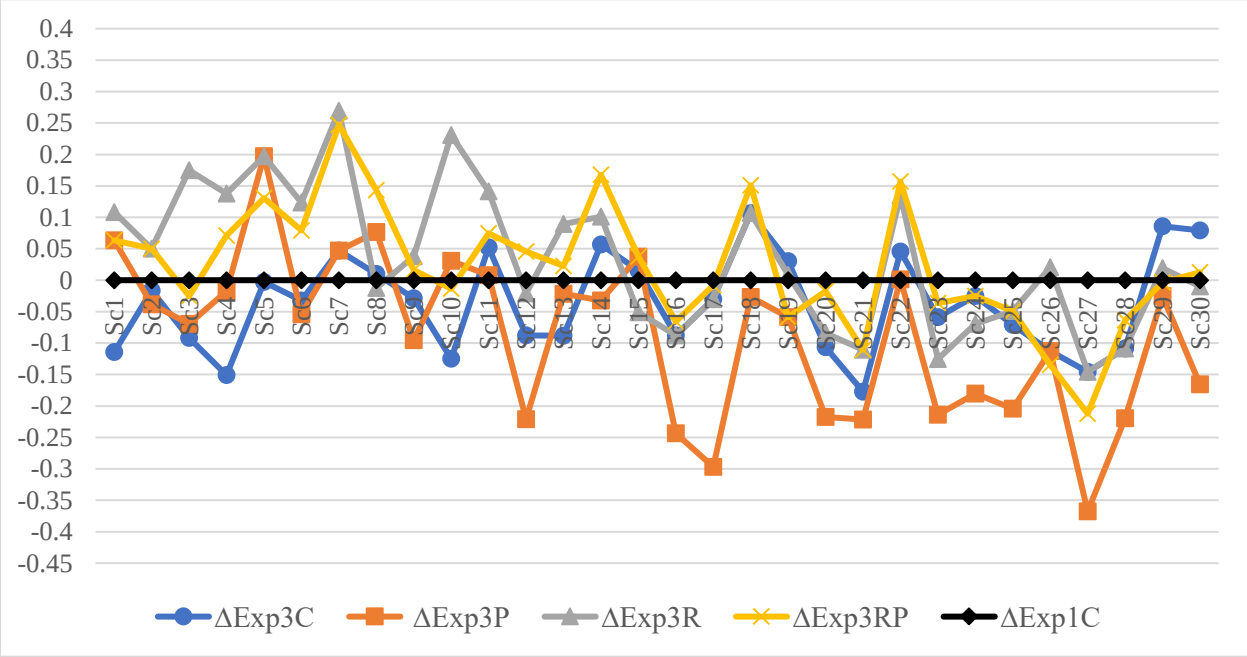

Figure 3 Exp3-I: Individual Reward and Punishment with Imperfect Detection

To simply control the scenarios' wording difference, Figure 3 used Exp1C as the subtracted base to illustrate the Difference of Compliance Ratio for all 30 scenarios in Experiment 3. Noticeably, a declining trend is presented even when individual reward and

punishment together was used. Comparing the line of Exp3C with the base (Exp1C), inferior compliance rates with larger magnitude are frequently displayed. Furthermore, comparing the line of Exp3P, Exp3R, and Exp3RP with Figure 1's Exp1P, Exp1R, and Exp1RP, respectively, the trends of reducing power of regulating noncompliance are also observed for all three pairs. This suggests that the effect of individual reward or/and individual punishment is gradually diminished under a large uncertain condition (20% inspection rate). All these findings further supported our hypotheses 4, 5, and 6.

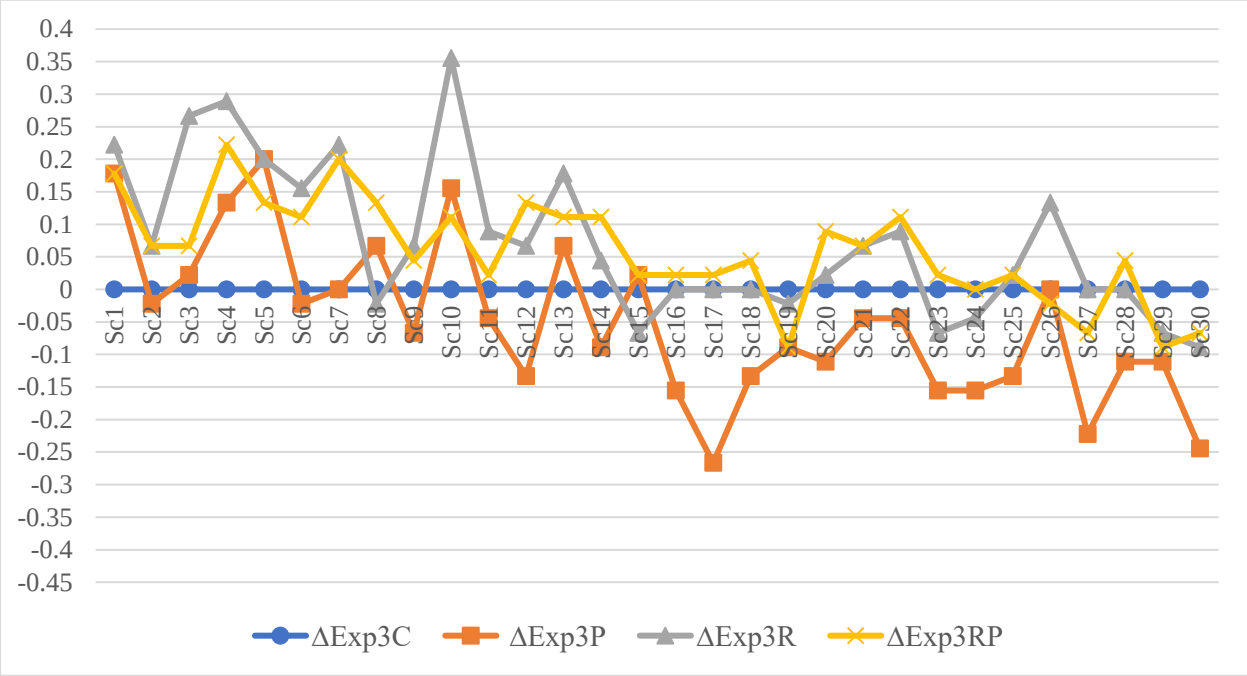

Figure 4 Exp3-II: Individual Reward and Punishment with Imperfect Detection

In order to further understand how individual reward differs from individual punishment under the low chance of being caught condition, Figure 4 shows the Difference of Compliance Ratio for all 30 scenarios in Experiment 3 when Exp3C is used as the subtracted base. Firstly, the same declining trend is still presented for individual reward or/and punishment after

controlling the detection effect (i.e., using Exp3C to partial out the scenario wording as well as a low-chance detection condition). Secondly, individual reward still outperforms individual punishment under the small inspection condition. This can be further demonstrated by the expected difference of Exp3R – Exp3P is 0.123 with a p-value less than 0.001. Moreover, the expected difference of Exp3R – Exp3C is 0.072 with a p-value of 0.031, which means that individual reward still has significant regulating power over noncompliance after controlling the detection effect. These two results are consistent with our finding in Experiment 1. A closer comparison between Figure 1 and Figure 4 seems to indicate that the regulating power of individual reward or/and individual punishment is shrinking (amplitude-wise) over time after controlling for the detection effect.

Interestingly, individual punishment with small inspection is no better than the control group with small inspection, as the expected difference of Exp3P – Exp3C is -0.050 with a p-value of 0.121. Meanwhile, individual reward and punishment together with small inspection is also no better than individual reward only with small inspection because the expected difference of Exp3RP – Exp3R is not significant with a p-value of 0.452. This could be explained by our common sense that law must be enforced, otherwise, no one will obey it eventually. When deterrence is uncertain to a large degree, the regulating power of punishment is often ignored over time by employees. This finding suggests a company needs to enhance its deterrence certainty in order to prevent insider data breaches if the punishment mechanism is adapted, although we found that punishment only is not effective to present noncompliance. Since individual punishment with small inspection is gradually disregarded, the complementary effect between reward and punishment is minimized. Hence, the effect of individual reward and

punishment together with small inspection is statistically no difference on average from individual reward with small inspection.

3.6.4. Experiment 4 and discussions

Our Experiment 4 is the most comprehensive and was designed to study how a low chance of being caught interacts with collective sanctions to regulate noncompliant behavior. The expected difference of Exp4P – Exp1C is negative (-0.123) with a p-value less than 0.001. However, the expected difference of Exp4R – Exp1C is 0.063 with a p-value less than 0.001 and expected difference of Exp4RP – Exp1C is 0.057 with a p-value of 0.018. These suggests that collective reward with a small inspection outperforms the most basic control group, which relies on employees' perceived obligation for compliance. But, collective punishment with a small rate of inspection is worse than the basic control group. The following Figure 5 may reveal the reasons and provide more details.

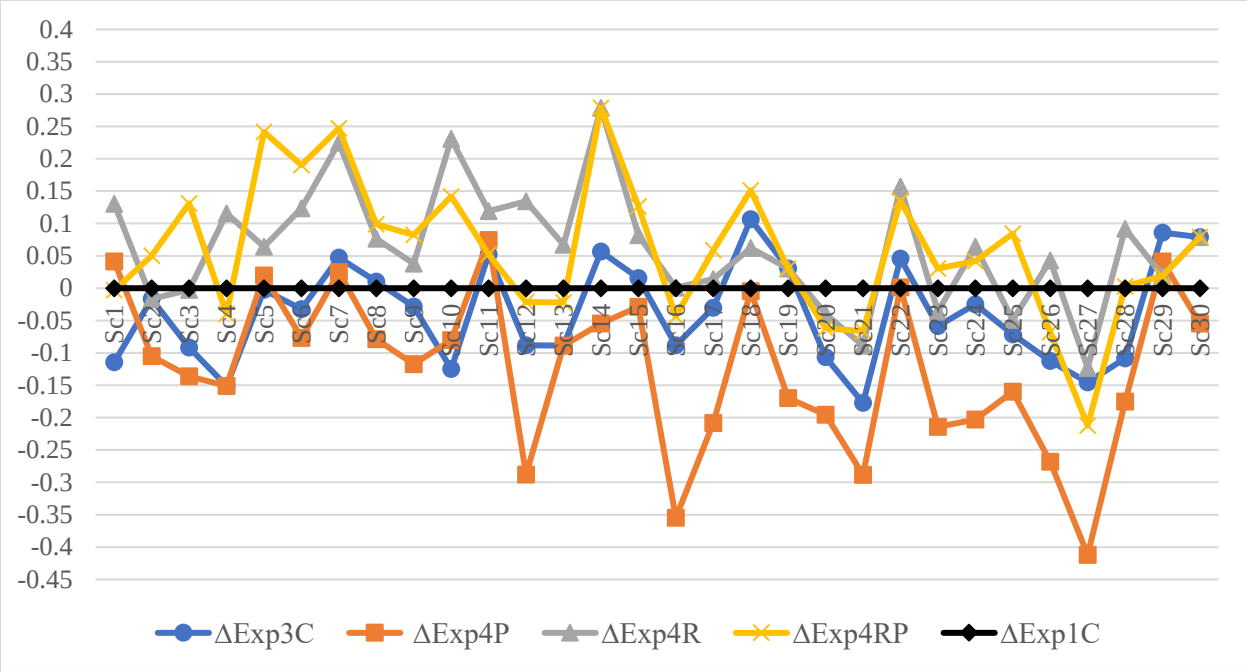

Figure 5 Exp4-I: Collective Reward and Punishment with Imperfect Detection

Figure 5 used Exp1C as the subtracted base to demonstrate the Difference of Compliance Ratio for all 30 scenarios in Experiment 4 to only control the scenarios' wording difference. A less rapid declining trend is observed compared with Figure 2. Such declining trend is inevitable because our collective sanction mechanism does not permit group members to target one another. However, the low chance of being caught (i.e. large uncertainty) delays the collapse of cooperation in information security compliance caused by the collective sanctions.

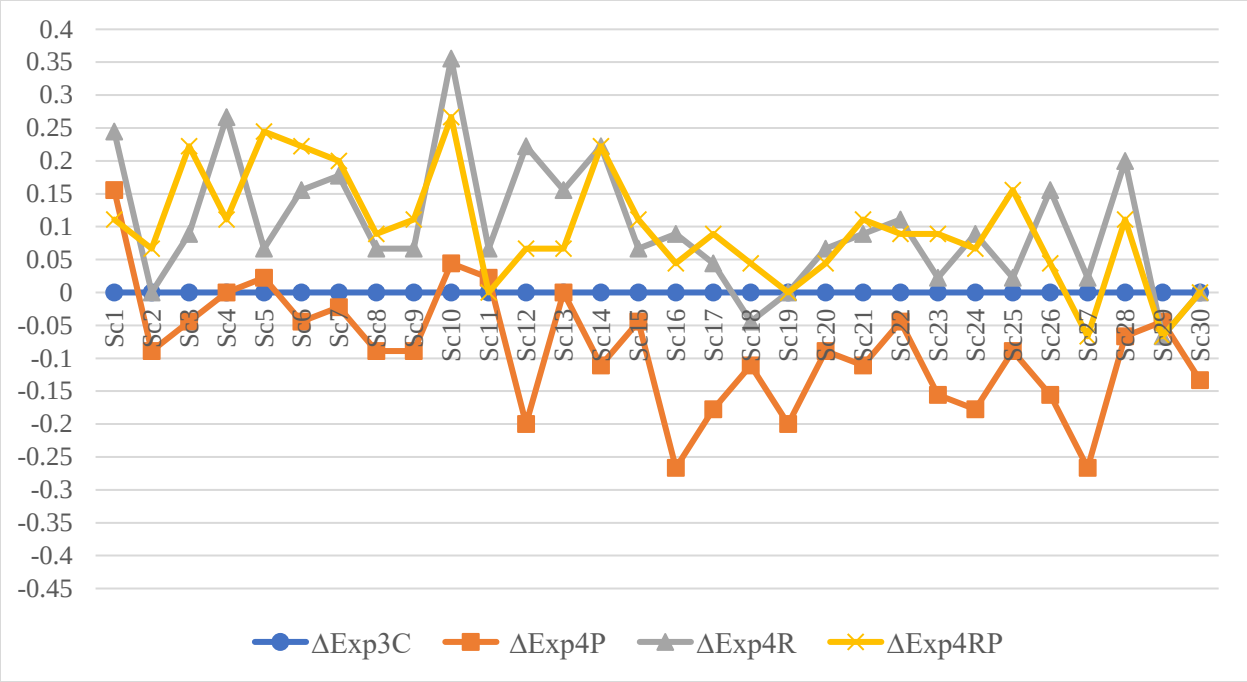

Figure 6 Exp4-II: Collective Reward and Punishment with Imperfect Detection

Figure 6 illustrates the Difference of Compliance Ratio for all 30 scenarios in Experiment 4 when Exp3C is used as the subtracted base for controlling scenarios' wording difference as well as detection effect. Although the declining trend is still presented for the collective sanctions under the small inspection condition, this non-compliance trend is also moderated and slowed down, compared to Figure 2. After controlling for the detection effect, the expected difference of Exp4P – Exp3C is also negative (-0.085) with a p-value less than 0.001, the expected difference of Exp4R – Exp3C is 0.101 with a p-value less than 0.001, and the expected difference of Exp4RP – Exp3C is 0.095 with a p-value less than 0.001. This means that collective reward only as well as collective reward and punishment together outperform the control group under the environment of a large uncertainty. But, collective punishment is worse than the control group when a low chance of being caught is present.

Although these are inconsistent with our findings about the general negative effect of collective sanctions in Experiment 2, when detection is certain; it is still very interesting to learn that collective reward is superior and collective punishment is inferior no matter the low chance of being caught is involved in the treatment or controlled in the treatment. This also demonstrates that the interactions between collective sanctions and low chance of being caught are not simple liner additive relationship, as both collective reward and collective punishment would be worse than the control group after controlling the large uncertainty influence. Rather, the low chance of being caught transforms the collective reward mechanism and differentiates its regulating power from the collective punishment.

In addition, after controlling for the detection effect by comparing Experiment 4 with Experiment 3, we can learn how the low chance of being caught changes the relationship between collective sanctions and individual sanctions. The expected difference of Exp4P – Exp3P is negative (-0.035) with a p-value of 0.012, which suggests that collective punishment is worse than individual punishment under the condition of a large uncertainty. This is consistent with a previous finding when the detection system is perfect. On the contrary, collective reward is slightly better than individual reward when a large uncertainty is present. This can be seen by the expected difference of Exp4R – Exp3R is 0.029 with a p-value of 0.114 (one tail is 0.057). Furthermore, the expected mean of Exp4RP – Exp3RP is also positive (0.037) with a p-value less than 0.001. This means that the collective reward and punishment together is better than individual reward and punishment together when a low chance of being caught is present.

In order to understand the fundamental reasons behind the above inconsistent results compared when detection is certain, we also compared Experiment 4 with Experiment 2. The only difference between these two experiments is the low chance of being caught. We found that the large uncertainty has a negative impact on collective punishment, but a positive impact on collective reward. These can be shown by the expected 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 expected difference of Exp4RP – Exp2RP is 0.041 with a p-value of 0.037. This indicates that the large uncertainty also has a positive impact on collective reward and punishment together. These results are consistent with the findings when the detection effect is controlled between Experiment 3 and 4. The following is our arguments why a large degree of uncertainty plays different roles between collective reward and collective punishment, as well as how it transforms collective reward from inferior to superior performance in enhancing compliant behavior.

Due to the low chance of being caught and uncertain punishment, people tend to commit more to security violations. This catalyzes the reciprocal selfishness and cultivates a negative atmosphere among group members, and hence facilitates the deterioration of cooperation in security compliance. Therefore, the low chance of being caught has a significant negative impact on collective punishment no matter if it is involved in the treatment (i.e., Exp4P vs. Exp2P) or controlled in the treatment (i.e., Exp4P vs. Exp3P).

Remember, punishment will be imposed on everyone, including compliant people, as long as someone in the inspection list is noncompliant. Whereas, reward will be given to

everyone including noncompliant ones, when all people in the inspection list is compliant. Therefore, the small inspection list (i.e., low chance of being caught) actually relaxes the very restricted small-chance condition (see the Experiment 2 and Discussions) required by our collective reward mechanism, although more people get rewarded even if they might be noncompliant. This reduces the tie-for-tat hatred among group members, as the chance of reward being incorrectly taken away from compliant ones is greatly reduced. Accordingly, the regulating power of reward is reserved and stands out. Hence, the low chance of being caught has a significant positive impact on collective reward, no matter whether it is involved in the treatment (i.e., Exp4R vs. Exp2R) or controlled in the treatment (i.e., Exp4R vs. Exp3R). Consequently, the complementary effect between collective reward and collective punishment is also reserved and enhanced due to the collective reward's outstanding, no matter the low chance of being caught is involved in the treatment (i.e., Exp4RP vs. Exp2RP) or controlled in the treatment (i.e., Exp4RP vs. Exp3RP).

Lastly, within Experiment 4, we also observed a couple of similar patterns as Experiment 3. Collective reward with small inspection outperforms collective punishment with small inspection. This can be found by the expected difference of Exp4R – Exp4P is 0.188 with a p-value less than 0.001. In addition, the expected difference of Exp4RP – Exp4R is not significant, with a p-value of 0.733; therefore, collective reward and punishment together with small inspection is no better than collective reward only with small inspection. This further demonstrates that reward is the preferred mechanism to regulate insider data breaches even in a collective form under the environment of a low chance of being caught.

3.7. Robustness, Demographic and Personal Characteristic Variables

We collected the participants' demographic and personal characteristic variables instructed by Hu et al. (2015)'s paper. In addition, we also employed the Holt and Laury (2002)'s risk aversion's measurement, as suggested by the risk taking and impulsivity survey construct adopted from Hu et al. (2015)'s paper. As aforementioned, in order to understand how demographic and personal characteristic variables influence participants' decisions for information security policy violation, we had to change the unit of analysis from treatment group level to individual person level. As each participant makes binary a decision between compliance ("No") and noncompliance ("Yes"), logit regression is used with encoding "No" as 1 and "Yes" as 0. In addition, clustered errors around the same participant is adjusted in the regression, because we coded dummy variables through 1 to 30 to control the potential effects caused by 30 different scenarios' wording. The following Table 3 shows the logit regression results for participants' compliance with information security policy.

Table 3 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)

Table 3 continued

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)
Gender: Male		0.0249	0.0833
		(0.196)	(0.185)
Gender: Female		0.0582	0.127
		(0.196)	(0.185)
Gender: Other		-0.0370	-0.0670
		(0.355)	(0.320)
Gender: N.A.		0	0
		(.)	(.)
Dominant Hand: Right		-0.0502	-0.0919
		(0.115)	(0.124)
Dominant Hand: Left		-0.0337	-0.0812
		(0.119)	(0.127)
Dominant Hand: N.A.		0	0
		(.)	(.)
Non-business Major		0	0
		(.)	(.)
Business Major		-0.00329	0.00148
		(0.0215)	(0.0221)
Computer Skills		-0.00958	-0.00791
		(0.0125)	(0.0127)

Table 3 continued

Class: Freshman	-0.0512	-0.0590
	(0.258)	(0.294)
Class: Sophomore	-0.103	-0.0954
	(0.257)	(0.294)
Class: Junior	-0.0690	-0.0566
	(0.256)	(0.293)
Class: Senior	-0.142	-0.125
	(0.255)	(0.292)
Class: N.A.	0	0
	(.)	(.)
GPA	-0.00890	0.00547
	(0.0103)	(0.0105)
Race: White	-0.0663	-0.0326
	(0.138)	(0.142)
Race: Hispanic/Latino	-0.0782	-0.0377
	(0.145)	(0.149)
Race: Black/African American	-0.0941	-0.0521
	(0.143)	(0.147)
Race: Asian/Pacific Islander	-0.0419	-0.0268
	(0.141)	(0.145)
Race: Other	-0.0579	0.0287
	(0.154)	(0.160)
Race: N.A.	0	0
	(.)	(.)
Organizational Experience	0.00998	0.00929
	(0.0137)	(0.0140)
Computer Hours	0.00898^{+}	0.00802
	(0.00531)	(0.00550)

Note: Marginal Effects (dy/dx) with Standard Errors in parentheses; N.A. stands for No Answer
$^{+}$ $p < 0.1$, * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

The most basic control group (i.e., Exp1C) was used as the base for categorical variable in the logit regression to test the treatment effects after controlling the scenario difference in the Model 1. Exp1RP, Exp2R, and Exp4P are significantly different from Exp1C for information security compliance. And Exp1R is weakly significant at 0.1 level for compliance as well. These results are consistent with our time series autoregressive model test for DCR. This is reflected by the same direction (i.e., sign) of numbers between the marginal effects of logit

regression and the expected difference of DCR (the first row of Table 2) in the time series data analysis. Careful readers may wonder why time series data analysis shows more significant value than the logit regression. This is because the standard errors for treatment effect are more precise when the unit of analysis of treatment group is used. As our research question is about the compliance behavior in workplace as group, using individual person as the unit of analysis for treatment effect is not appropriate, although it can permit us to study the individual difference for compliance. Furthermore, the standard errors caused by other unobserved variables of individual difference shall be averaged out when we use the treatment group as the unit of analysis, which shall provide more accurate statistical test results for treatment effect.

The logit regression with demographic and personal traits variables is presented in Model 2 of Table 3. Interestingly, the significance level and the sign of marginal effects did not change much, except Exp1R is significant from the 0.1 to 0.05 level and Exp3P becomes 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 our robust results of time series data analysis, as it did not incorporate those demographic and personal traits variables for examining the treatment effect.

In addition, risk taking is negatively significant at 0.001 level. This suggests that risk-loving employees are more likely to violate information security policy. Furthermore, impulsivity is also negatively significant. Impulsive people was defined by Hu et al. (2015) as the individuals who do not take adequate time to evaluate input before making a decision. Hence, it makes sense that impulsive employees tend to violate information security policy more

due to the time-saving characteristic. Moreover, age is another significant factor for security compliance. The positive coefficient of age suggests that the older employees are more likely to comply with information security policy compared with younger ones.

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 the average hours of using computers per day seems to have a weak effect. This may very well explain why insider data breaches happened so frequently no matter the workplace environment (e.g., companies, governmental sectors, universities, or other nonprofit organizations). It is worthy to note that business major students are no different from non-business major ones for information security compliance. This demonstrates that our data collection is unbiased for gathering two populations.

Unexpectedly, the Holt and Laury (2002)'s risk aversion's measurement is not significant in Model 2. We suspected that this may be caused by its multicollinearity with risk taking and impulsivity, as risk aversion is a very similar construct with previous two in an opposite way. Hence, we omitted both risk taking and impulsivity in Model 3. Then, risk aversion becomes weakly significant with a positive sign of marginal effect. The positive value matches to our intuition as well as risk taking's result that risk-averse individuals are more likely to comply with the information security policy. In addition, Model 3 represents the almost same regression results as Model 2 even without two significant factors. This further proves that the demographic and personal traits variables are independent from the treatment variables for

information security compliance. Therefore, it further demonstrates the robustness of the results concluded from our time series data analysis.

3.8. Conclusions, Implications, and Limitations

Information security is an undebatable important question for both academic research as well as industry practice. Although so much effort has been put into this topic through various means including technological defense as well as regulating policy, data breaches seem to become more and more common and hard to prevent. Much literature has identified that human factors, particularly employees' noncompliance with the information security policy, are the fundamental causes for data breaches, as insider employees are the weakest spot for security defense.

Our paper aims to design a realistic incentive structure to help a company to better protect its information assets. To the best of our knowledge, our study is the first attempt through the lens of behavioral economics to explore how individual sanctions, collective sanctions, and detection influence employees' compliance with a company's information security policy. The nature and complexity of individual reward, collective reward, individual punishment, collective punishment, a large uncertainty, and their interactions were gradually unfolded through a series of sequential lab experiments. Furthermore, we illustrate that a few noncompliant behaviors are fatal to the security defense of a company, especially under the current Internet era. Hence, how to regulate such noncompliance and "induce" cooperative compliant behavior is even more critical for a company's long-term benefit. After the thoroughly discussions of our experimental results, we have the following major conclusions.

Firstly, individual reward and punishment together with certainty is the best strategy for a company to regulate its employees' noncompliance. This can be clearly evidenced by the dominant superior performance of Exp1RP in Table 2. In a broader setting beyond the information security, temper justice with mercy or carrot and stick has hundreds of years of usage history for preventing social undesirable behavior and cultivate the wanted behavior. The complementary effect between reward and punishment is very strong, and thus omitting either one could be a considerable managerial mistake. Therefore, in the long run, a company shall always employ both means to achieve better regulating power, although it may cost the company some capital for rewarding.

Secondly, individual reward is always better than individual punishment for intensifying security compliance. This suggests a company shall rethink about their managerial policy which 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, as the employee wants more work done but the company wants more work done securely. In addition, the modern fast-pace life style may make employees pursue more self-interests and short-run benefits. Hence, giving a reward for compliant behavior aligns both parties' interests.

Thirdly, collective sanctions are a complex incentive mechanism. A company should use it with great caution. In general, collective sanctions have a spiral-downwards impact on cooperative compliance when interactions among employees are not permitted. For a large size

company with loose social ties including blood bonds among employees, it would be very dangerous to adopt collective sanctions mechanism to regulate noncompliance. Punishing all due to a few noncompliant ones may cause rebellion and hatred culture in the workplace. Meanwhile, rewarding all becomes a small-probability event as the size of group members is large. Thus, employees' motivation for pursuing the collective reward is dramatically reduced. Instead, a company may try the collective reward to those small departments or groups which have a strong interactive atmosphere. Furthermore, different cultures may have different results when collective sanctions are used. It might be reasonable to argue that collective sanctions are better supported by collective cultures than individual cultures. A company with a collective culture may be able to better utilize the collective sanctions to achieve its positive potential pointed out by Heckathorn (1988).

Fourthly, a large uncertainty or small inspection rate undermines the incentive power of individual reward or/and individual punishment. Hence, a company must improve its detection systems in order to take full advantage of individual sanctions. This requires the joint effort between a company's technical team and managerial leadership. In addition, uncertainty has a stronger negative force to weaken punishment, as the deterrence is not fully enforced. A company is better off to either not use punishment or make it certain; otherwise, punishment with uncertainty is even worse than employees' own moral/ethical obligations. Therefore, in the real workplace with a small inspection or very low detection accuracy, the company should always avoid using a punishment only mechanism no matter in individual form or collective form, but use it only when rewards are also present.

Lastly, examining through our four experiments, we find that the superior complementary effect between reward and punishment is always observed no matter in individual form or collective form. In addition, a company is also advised to avoid hiring risk-loving, impulsive, and junior people (if possible) for the key information security positions. Because those employees may pose a stronger threat to a company's security defense and their compliance may not be easily improved by rewards or/and punishments no matter in what forms.

CHAPTER 4. THE APPLICATION OF BLOCKCHAIN IN ADVANCING INFORMATION SECURITY

4.1. Introduction

In the era of big data, information assets are one of the most valuable intangible productive capital for a company to compete with its rivals, to learn consumers' shopping habits, to guide its development directions, and to standout to retain its profitability. However, with the Internet's characteristic of pervasiveness, information breaches from both external hacking and internal corruption are continuously encroaching a firm's economic profit. In 2013, *The New York Times* reported an international cybercriminal group had stolen up to $1 billion from more than 100 banking and financial institutions in 30 different countries around the world. More concerning, these cyberattacks continued for two years without detection by banks, regulators, or law enforcement (Sanger and Perlroth 2015). In the same year, Target's payment network system was intruded via its third-party vendor, Fazio Mechanical Services, a provider of refrigeration and HVAC systems according to CNN news (Wallace 2014). More importantly, so many corporations or organizations are constantly dealing with data breaches without announcing it to the public. This is mainly due to the firm's self-protection of its brand reputation and fear of letting the public know its failure of protecting its customers' information. Hence, securing information assets has become one of the top concerns of a firm's future developing strategy. Although information science, computer science, and other related disciplines have developed advanced tools to protect information assets, hacking activities grow worse by the day. We cannot help but to ask ourselves: "Why?" Are there any problems about the fundamental design of our current information security models? In this conceptual article,

we introduce the breakthrough idea, Blockchain, the first native digital medium for securely transferring value over the Internet (Tapscott and Tapscott 2016). Furthermore, we rely on the Theory of Bounded Rationality to discuss how Blockchain technology can undermine the motivations of intruders in order to prevent information breaches.

4.2. The Theory of Bounded Rationality and Information Security Defense

Rationality is widely used as the core assumption for studying individual behaviors in microeconomic models. It assumes that one shall always behave selfishly. Rational Choice Theory in economics further explains that an individual has preferences among the available choice alternatives that allow them to state which option they prefer (Tversky and Kahneman 1986). Accordingly, the rational agent is assumed to consider all available information and potential costs as well as benefits in determining preferences, and to act consistently in choosing the self-determined best choice of action. Rational choice theory also assumes that an individual has a well-organized and stable system of preferences, and is capable of finding the highest attainable point on a preference scale among all alternative choices. Herbert A. Simon (1955) instead argues that humans are limited for the tractability of the decision problem, the cognitive limitations of his minds, and the time available for him to make the most optimal decision. When an individual uses heuristics to make decisions rather than a strict rigid rule of optimization due to his inability to process so many complex alternatives, this is so call Bounded Rationality. This Theory of Bounded Rationality has been widely used in economics, political science and related disciplines for its practical view of human rational (Gigerenzer and Selten 2002). However, for protecting information assets and preventing data breaches from a managerial perspective, bounded rationality is underexplored.

The classical approach to information security defense is to employ the principles of *defense in depth* and *least privilege*. Those principles stand from a technical view of information security to block an attack by layers of redundant defense mechanisms, and restricting users' (e.g., employees') privilege to access protected information so as to prevent breaches. Even with a best-effort application of contemporary technology supporting these two key principles, data breaches still happen. In this paper, we turn our attention to the motivation of the attacker rather than focusing on mechanisms to prevent unknown assailants.

As both external hackers and insider employees are human beings with bounded rationality, a better defense system could utilize the nature of limited cognitive capacity of human beings to undermine intruders' motivations for data breaches. In other words, a defense system by leveraging human's bounded rationality to force intruders to compliance with the system rather than break into the system would be the ultimate solution for information security.

4.3. Motivations and Incentives for Data Breaches

The famous criminal Willie Sutton was once asked why he robbed banks, Sutton replied, "because that's where the money is." One may wonder why few persons rob the federal reserve banks nowadays. This is because the robbers' bounded rationality that they have limited resources and capacity to execute their robbing plan. Data acts like "oil" in the digital economy and "fuel" its respective corporation to operate. Hence, it is extremely critical for a company to secure its data from tampering and maintain the access to its data for uninterruptible usage. On the other hand, when valuable things are protected in multiple locations, it is extremely costly for

the protectors to operate, at least this is true for physical treasure. Hence, firms are constantly facing data breaches as their data is valuable and centrally protected.

Practically, money has no value if it cannot be traded for other things. The same is true for data as well. Stolen data are profitable for intruders when they can be exchanged or sold to others for monetary gain (e.g., credit card information), when they can be tampered or manipulated for malicious purposes (e.g., governmental secrets), and when they can be leveraged or utilized for threatening (e.g., private records). If there is no demand, supply will decrease over time. For example, email accounts used to be very profitable stolen information (e.g., $4 ~ $30 per account in 2007) for intruders as one's email may contain valuable information such as disclosing logins to other important online services (Wueest 2015). By 2015, the price for 1,000 stole email accounts has dropped to as low as $0.50. Instead of stealing email accounts, more and more identity related data breaches (e.g., medical information) occur in recent years as they are more profitable for hackers. According to McAfee Labs Report (McFarland et al. 2015), the sale of a victim's identity information is the most frightening and profitable among all categories in current data breaches. Credit card with full personal identifiable information including social security number, mother's maiden name, and date of birth is worth of $30 per account in the black market. Even worse, some hackers demanded a ransom of €20,000 for threatening to disclose Labio (a French medical-service provider) patients' diagnostic test results publicly. As data breaches keep happening with different forms, we believe the new way of thinking to prevent data breaches is to employ an approach which may eventually undermine those motivations of intruders for hacking data centers.

Accordingly, there are three main categories for intruders' motivations: monetary gain, political purposes, and emotional incentives. Emotional incentives could include the revenge motivation of an disgruntled employee, mischievous motivation because of curiosity, and self-actualization of a sophisticated hacker. Political hacking could include a governmental sponsored effort. Monetary gain, especially for online-bank data breaches, is the major motivation for data breaches (Peretti 2008). Monetary-gain data breaches can have multiple forms. Hackers may attack the banking systems directly or steal financial and identity information from other industrial sectors (e.g., hospital). In October 2014, JP Morgan found about 76 million households and 7 million businesses were compromised including names, addresses, phone numbers, email addresses, and others (Glazer and Yadron 2014). Additionally, in May 2015, Anthem was attacked and about 80 million current and former customers' information was stolen. That information was sold for profit for fraud, identity theft, and even blackmail (Mathews 2015). In December 2016, Yahoo announced more than one billion user accounts had been compromised since 2013, which is one of the largest data breaches until now. This attack involved sensitive information including names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions that could be used to reset a password (Goel and Perlroth 2016).

In this paper, we focus on those intrusion activities based on monetary gain although the other two motivations for intrusions are also important. We believe cutting off intruders' avenue of cashing out stolen data is the key for future information security strategy. The following will discuss how Blockchain technology with cryptocurrencies will help to protect the financial

industry, then we will extend the discussions to other industry that how Blockchain could assistant and advance current information defense systems.

4.4. The Value of Currency and the Value of Digital Assets

Historically, trade is established because of the needs of exchange, and money exists to facilitate such trade between people. Through the centuries, trade has become incredibly complex across regions. Everyone trades with everyone worldwide. Instead of the old-fashion of carrying gold around, modern local government issues physical money to safeguard the trade among unfamiliar parties within its span of control to securely facilitate the trade. Trade is then recorded in bookkeeping, where the information is often isolated and closed to the public. Hence, people use third parties and middlemen they trust to facilitate and approve their transactions. Accordingly, the bank system is established to do such tasks. In ancient times, we assigned the privilege only to those people who we can mutually trust to handle our wealth and build a solid "wall" as well as use guards to safeguard against thieves. In the modern time, our wealth is abstracted as a number in the bank's private database which is secured by advanced information technologies. Physical currency is valuable because it allows us to spend to fulfill our needs. It is secured by the local government from counterfeiting and prevented naturally for double spending as a physical being. Complementarily, our current e-bank systems are just the digital representation and extensions of the physical bank systems developed historically. Accordingly, it still requires the trusted third parties (i.e., banks) to perform trades even for on-line transactions, audit one's financial account from fraud, and prevent double spending issues through the central clearing house.

The value of a paper note is defined by the contemporary market although the number printed on it never changes. The ownership of the paper note is secured when one possesses it. Most of the time, the value of physical assets can be quantified and abstracted as an amount of local currency. The same principle is also true for the digital assets. Its value is assessed by current market and secured by its respective ownership via technological protection in the digital world. However, due to the zero cost of duplication of digital assets, the value of the digital assets cannot be easily transferred without an appropriate way of transferring ownership. Instead, their value may be diminished quickly with the number of replications. In fact, in some cases like trade secrets, its value will be stolen completely when the original information asset is leaked out. Therefore, Bitcoin, a digital cryptocurrency, was developed to secure virtual-currency transactions over the Internet. Furthermore, with the Internet's pervasiveness, Blockchain technology, the underneath-supporting infrastructure of Bitcoin, was generalized for securely transferring value in the digital world.

4.5. Blockchain and a New Way to do Bookkeeping

There is no clear origin of the concept of Blockchain, but its first application, Bitcoin, was published in 2008 by Satoshi Nakamoto. Bitcoin is a purely peer-to-peer version of electronic cash, which allows online payments to be sent directly from one party to another without going through a financial institution (Nakamoto 2008).

In a regular financial institution, bookkeeping is the foundational stone of its operations to record transactions. Each financial institution (e.g., individual banks) has its own private ledger and a proportion of that ledger is made publicly for the central governing institution (e.g.,

clearing house) to allow communications and broad transactions. On the other hand, Blockchain is the underlying distributed general ledger of Bitcoin for recording that a transaction happened, when it happened, and that it happened correctly, without exposing any confidential details about the subject or the parties involved (Deloitte 2015). Specifically, it is a vast globally distributed ledger or database running on millions of devices and open to anyone to access and audit who are on the Blockchain network. Entries in the database are configured in "blocks" which are then chained together using digital, cryptographic signatures. In the Blockchain ecosystem, trust is established not by powerful intermediaries like banks, governments and technology companies, but through mass collaboration and clever code (Tapscott and Tapscott 2016). This is a key property of Blockchain applications.

4.6. Blockchain and its First Application, Bitcoin

Bitcoin is different from the paper currency issued by governments to facilitate trade. Specifically, Bitcoin, at the basic level, is just a ledger with account numbers and balances with its owner's "private key." It may sound like one's online bank account, but the ledger of Bitcoin is owned by everyone in the Bitcoin network, not just one person's bank systems. One may feel uncomfortable that others may know his account information; however, the design of Blockchain cleverly resolves such concerns with a pair of keys that generated by the Elliptic Curve Digital Signature Algorithm (Bos et al. 2014). A digital signature is a kind of one-way cryptographic puzzle that only the owner of the Bitcoin can solve because only she/he holds the key that generates the digital signature with hashing operation. This is so-called "private key" which should be kept secret by its true owner. The other half of the digital signature is called "public key", which is calculated from its respective private key and such mathematical operation is not

reversible. It is used by others to check whether the signature is genuine. The public key can either be used raw in a transaction, or converted into a Bitcoin address by means of hashing and other operations to preserve anonymity. The combination of a hacker's bounded rationality and the complexity of the underlying cryptography makes it practically impossible to crack one's private key as long as the private key is randomly chosen.

There are three types of Blockchain infrastructures in current practice: public/open, private, and governmental (Mueller-Eberstein 2017). Private and government controlled Blockchain networks are closed to the public and participants must be approved. Accordingly, the speed of processing transaction is faster and typically the identities of involved nodes are known to the owners of the Blockchain infrastructures. For example, Citibank has been experimenting its own version of digital currency, CitiCoin, within its own controlled network (Popper 2015). Disney also invents its own Blockchain platform, called Dragonchain (McKendrick 2016). The Dragonchain aims to create cost-efficient business networks where virtually anything of value can be tracked and traded. On the governmental side, Estonia is one of the earliest governments adopting Blockchain technology to facilitate citizen interactions with the state through the use of electronic solutions (Walport 2016). e-Estonia the Digital Society offers many e-services through its Blockchain network including i-Voting, e-Tax Board, e-Business, e-Banking, e-Ticket, e-School, and e-Governance Academy (Scott 2014). Its website states, e-Estonia "opens the door to all secure e-services while maintaining the highest level of security and trust"(Estonian 2017). In Asia, the People's Bank of China also heavily invests in Blockchain technology including its own version of digital currency (Popper 2016a).

In contrast to closed networks, the public/open Blockchain embraces everyone who wants to join in the network through the Internet. It is permissionless and secured by proof-of-work, which is a piece of data that is difficult (costly and time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Because all participants on the network need to verify transactions and update local copies of the ledger in a globally consistent way, public Blockchain transactions typically takes longer to process. Bitcoin is not only the first application of Blockchain, but also the most successful digital currency utilizing the public Blockchain infrastructure (Popper 2017). Ethereum is another well-known application of public Blockchain which focuses on embedding smart contracts into Blockchain system (Popper 2016b). In this paper, we focus on the public Blockchain mechanism as other types are just derivatives.

To illustrate how a fund transfer works in the Blockchain infrastructure, the transaction begins when the originator broadcasts to all network participants that funds are being transferred. The message includes the account numbers to be credited and debited, and the amount of the transfer. Then, other computers or nodes in the Bitcoin network apply that transaction to their copy of the ledger and pass on the transaction to other nodes that have not yet received the message from the originator. Eventually, everyone on the Bitcoin network will have the same copy of entire ledger; hence, it creates a system that lets a group of computers/entities maintain a ledger instead of a bank's private network. Unlike at a bank where you only know about your own transactions, everyone in the Bitcoin network knows about everyone else's transactions. In order for ensuring that the request of changing the transaction is authentic and only the rightful owner has sent the message, unlike a simple static password, a completely different digital

signature is required for every transaction (Driscoll 2013). The Bitcoin owner needs his private key to create a transaction signature and others need the public key to check the validity of the on-going transaction. The digital signature is unique among all transactions as it is generated by the owner's private key with hashing the message itself. Any attempted changes to the original transfer message will result in a completely different digital signature and the attack is therefore detected. If the transaction is verified by miners (i.e., participating computers of processing Bitcoin transactions), it will add a new digital signature to the Bitcoins, which can be completed only by its new owner. All miners work independently on their own version of the Blockchain to make sure the signature is correct and have enough Bitcoin balance to make the transactions (i.e., prevent double spending issues in the digital world); then they bundle the new records into a block and add it to the end of the Blockchain (Peck 2015).

Hence, the ledger in a Blockchain is essentially a long-string of transaction records, each of which refers to an earlier record in the chain. The arrangement will only converge when the miners agree on what the most recent version of the Blockchain should look like (Peck 2015). Because the process of adding a new block of transactions to the Blockchain is very difficult and it is designed that anyone who participates is required to devote a large amount of computing power and electricity towards running the new data through a set of complex math calculations (e.g., hash functions). The complexity of the computations and the many copies of the ledger make it very difficult for an attacker to change the distributed Blockchain ledger without nearly complete collusion.

4.7. Blockchain and Its Properties

There are several key properties of the Blockchain ecosystem (Murck 2017) that make it interesting to consider in the context of improving information security. First, *distributed nature of structure to eliminate trusted third parties*. At the most basic level, Blockchain is very similar to the distributed database. Each database has a full copy of original data, and any changes in one database will be synchronized across the others. Instead of one or a few trusted third parties control the distributed database, everyone on the Blockchain has access to the entire database and its complete history, although the database is encrypted and accessible by its respective software only. This breakthrough design allows Bitcoin to be used across multiple nations without banks and clearing houses.

Second, *peer-to-peer transmission without the need of middle parties*. Transactions over Blockchain network are peer-to-peer without going through the trusted nodes. This allows the value transfer of digital assets quicker, faster, more efficient, and more secure as the vulnerability of middle parties are removed completely from hacking. Accordingly, the likelihood of data breaches is greatly reduced.

Third, *transparency with pseudonym preserving information privacy*. Transactions over the Blockchain are identified by one's public key, which is not associated with his identity. Furthermore, users on a Blockchain can choose to hash their public key and turn it into a blockchain address to further mask their private information, although every transaction and its associated value are visible to anyone with access to the system. The hash function ensures the mathematical operation is one-direction conducted and non-invertible. There is a unique link

between the hashed content and hash values; hence, user's transactions are only theoretically traceable over blockchain although they may be hashed multiple times. Accordingly, it might be possible for a hacker to identify a target over the Blockchain network, but based on the theory of bounded rationality and the enormous searching space behind the traces, hackers are not incentivized to do such attacks.

Fourth, *immutable from tampering*. This property is the core principle for Blockchain in advancing information security. Once a transaction is agreed by miners, entered in the general ledger, and respective accounts are updated, the records cannot be practically altered, because they are linked to every previous transaction one by one through the chain. Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, time stamped, chronologically ordered, and available to all others to verify over the Blockchain network.

Lastly, *computational logic to enable auto-execution*. Blockchain is a digital ledger and thus inherits the program-enable nature of computational algorithms. In other words, blockchain transactions can be tied to computational logic and in essence programmed to execute certain codes when the conditions are met. Accordingly, certain rules and policy can be embedded into Blockchain network to ensure the intended tasks will be performed without malicious interfering. For example, the name of recipients or specific transaction rules can be easily programmed into the Bitcoin (so-called compliancy up front). The unit of Bitcoin can even be programmed in such a way that it will automatically return to the sender if the receiver does not match to the on-

file records. Hence, such property can largely reduce the data breaches from both insider and outsiders as the compliance is put in place prior.

A common approach to secure digital assets is to build walls to lock people out of the network/system and hand out encryption keys only to those people who are permitted to access the certain information. The centralized control of protection of information assets is actually equal to the central point of failure of protecting, as the controlling node becomes the common target for attackers. Moreover, such centrally controlled mechanisms cannot ultimately prevent sophisticated ones to break in, but instead leave a natural shelter for the hackers to hide themselves among public as the public do not hold a copy of the ledger to verify thereby to reject tampering. Therefore, the properties of distributed mechanism and immutability of Blockchain can greatly improve current information security defense against external hackers' attack. In addition, since each unit of the content digitally stored on the Blockchain network can be programmed and auto-executed by the smart contract, and such execution is autonomous without middle parties, the properties of computational logic and peer-to-peer transmission thus can greatly prevent insider data breaches including both unintentional and intentional ones. The following sections further illustrate how those properties of Blockchain can help to assist and advance information security defense.

4.8. Blockchain Helps Prevent External Hackers

Although firms are increasingly spending more on developing better ways to protect information assets, hackers are becoming more sophisticated to break into the firms' systems driven by their motivation of "profit." There is no end for such battle between firms and hackers

as both parties are constantly improving their skills to either defend or attack. Hence, in order to prevent such data breaches, our economic society needs to reverse hackers' motivation for hacking. In the old security model, the system tries to lock out all of selfish and dishonest people. On the other hand, Bitcoin in the Blockchain system welcomes everyone to fully act in their own self-interest and then the system uses their selfishness to secure the network. The Blockchain, then, becomes more secure as more people participate in the network. Hence, Bitcoin causes an attacker to be better off by playing along than by attacking it due to the bounded rationality, since the incentive systems in the Blockchain leads a lot of people to contribute resources towards the welfare of the system (Eyal et al. 2016).

If we treat every online in-and-out activity of a firm as a transaction, the only way to confirm the absence of a transaction is to be aware of all transactions (Nakamoto 2008). In other words, the new security model cannot rely on any single trusted entity, especially the firm itself, to be aware of one's all transactions. Instead, all transactions must be publicly announced; hence, everyone knows everyone else's transactions including its capital and material flow.

As monetary gain is the main focus in this paper for hackers' motivation, thus hacking financial industry directly for profit is discussed first. In a traditional online bank system, people's financial assets (e.g., checking account, credit card, etc.) are protected, essentially hidden, by the bank's information technology. Online transactions with critical information are typically encrypted and securely transmitted over the Internet. The servers of the bank system which stores customers' financial information are also heavily guarded physically (e.g., security personnel and surveillance cameras) as well as virtually (e.g., firewall and intrusion detection

systems). But JP Morgan was still compromised in 2014. This is because once hackers successfully breached the bank systems and gain a control of the system, they could easily move funds to their desired destinations such as overseas. Hence, the rational choice for such sophisticated hackers is to keep hacking; once they can see the "gold", they will be able to move it. If a certain mechanism can bound hackers' rational choice by infinitely increasing the difficulty to move the "gold" even though they "see" it, then the hackers accordingly would have no incentive to attack those servers. Fortunately, Blockchain technology can effectively build such "transparent" wall to protect the "gold". Hackers can attack the Bitcoin network or a certain node on the network; if they are successful, they may be able to see one's Bitcoin account. However, when they attempt to relocate the victim's Bitcoins, they have to use the victim's private key to sign the digital signature in order to broadcast the sending-money transaction message over the Bitcoin network. This is different design from the traditional online bank, where a password is not required to move fund although it is needed to access one' bank account.

Moreover, most (if not all) digital wallets require two-factor authentication to access one's Bitcoin account. One's private key can be stored in the digital wallet protected by a user defined password or simply be written on a paper secured by its owner physically. As long as the private key is safely maintained, there is no way for hackers to move one's Bitcoin even though his digital wallet is compromised. Combined with current cutting-edge information security defense systems with Blockchain mechanism, the future financial industry can greatly increase the complexity to prevent a hacker's attack and thereby better protect their customers' financial assets.

In addition, in other industries, like music or software, the valuable digital assets stored on the Blockchain network can also prevent a hacker's monetary gain indirectly. In the traditional music industry, audio files (e.g., MP3) are stored in the company's servers and centrally protected. Hackers will be able to steal its music for profit as long as they successfully break into the company's database. Afterwards, the hacker will be able to duplicate the music and resale it for pirates. Since the transaction history of stolen music is not complete, the music producer company cannot effectively take legal actions to accuse music pirates. On the other hand, if the company stores its music on the Blockchain network, all music transactions will be recorded on the general ledger and the ownerships of the music are permanently written into the blocks. Thereby, legal actions can be effectively utilized by the music producer if pirates occur.

Accordingly, due to the fear of legal penalty, few people demand to pay such stolen music, and thus, supply will be reduced naturally. Eventually, such hacking of information assets would be diminished over time.

Furthermore, a hacker may be hired by a third party and thus gain profit by tampering with the sensitive data. However, the distributed nature of Blockchain ensures the data stored on it cannot be altered. Every node on the Blockchain network has a copy of the unpolluted data. Any modifications of the original data made by the hacker cannot be realized unless every node comes to the consent but nodes are synchronizing in real time. Theoretically, hackers may be able to tamper the data when they can change the existing records of Blockchain on more than 51% nodes at the same time. Fortunately, verifying, changing, and modifying the records require a large amount of computing power due to the mathematical calculations, which also means the

electricity power; hence, it is most unlikely for a hacker to pay such huge effort to manipulate the sensitive data. Accordingly, data integrity is secured through the Blockchain technology.

Data availability is another aspect of information security. In recent years, a new form of cyberattack, Distributed Denial of Service (DDoS), occurs frequently. DDoS occurs when hackers flood the servers that run a target's site with internet traffic until it stumbles or collapses under the overwhelming load. On October 21, 2016, millions of internet users across the U.S. were not able to reach several major websites including Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times (Perlroth et al. 2016). The reason was a massive DDoS attack that brought down the Domain Name Servers (DNS) of service provider Dyn, which supported major internet clients. Particularly, millions of internet-connected devices (so called the Internet of Things), which were infected by malware due to their poor security features, were used as launchpads to flood Dyn's servers. Such DDoS attacks are profitable for hackers who demand ransom from the victims. Interestingly, the Blockchain mechanism is very similar to the DDoS mechanism regarding their distributed nature. Instead of using Internet of Things as attacking launchpads, those devices on the Blockchain may become defense modules. If the DDoS targeting servers are also distributed through the Blockchain network, the overwhelming traffic caused by the DDoS attack would be divided over the Blockchain network. Thus, no single server (i.e. no single point of failure) will be flooded as the traffic has been scattered. Even if hackers are able to manage the DDoS attack for just targeting one or a few servers on the Blockchain at one time, the rest of servers, which are synchronizing in real time with one another, would be able to take turns to serve the company for its continuous use.

Lastly, Blockchain mechanism can also enhance current security countermeasures. A traditional system alarm (e.g., Intrusion Detection Systems) may not be sensitive enough to be triggered by a sophisticated hacker "quietly" cracking the protection system. However, if such a defending system is employed over the Blockchain network, any bit changes of system components will be easily identified through the pre-stored hashing values on the Blockchain and thereby raise an alarm for the system administers to take appropriate actions immediately. In addition, if multiple protection systems are used over the Blockchain network, the protection mechanism becomes robust and resistant for a hacker's attack as illustrated in the DDoS attack. Therefore, the Blockchain technology does not only prevent an external hacker from cashing out the stolen data to undermine his motivation, but also complements current security countermeasures to enhance the defense system. Thus, it greatly increases the complexity and difficulty with less incentives for a hacker to attack. Limited by his bounded rationality, current information security models are greatly improved with the application of Blockchain technology.

4.9. Blockchain Helps Reduce Insider Breach

Not all information systems are strong enough to prevent insider breach or intrusion if an insider betrayer colludes with an outsider intruder. The ongoing PwC survey in the UK shows that 75% of information security breaches in large organizations were caused by human factors in 2015 (PwC 2015). This figure is an increase from 58% compared with one year ago. In addition, the Kroll Global Fraud Report shows that 79% of fraud is perpetrated by insiders (i.e., employees) rather than by external hackers (Kroll 2016). The following discussion will explain how Blockchain can reduce insider data breaches due to employees' ignorance of security policies and their malicious actions in the workplace.

The major motivation of an employee to not comply with the information security policy to protect his company information assets has been identified as time saving (Puhakainen and Ahonen 2006). Employees feel frustrated when added security procedure slow down their work performance. In the financial industry, Blockchain has greatly reduced the inefficiency of trading and settlements by eliminating middle parties (Catalini 2017). In the supply chains industry, Blockchain has facilitated fast delivering and more efficient resource use for all partied involved in the supply chain systems (Casey and Wong 2017). The efficiency improved by Blockchain technology can relieve employees from time pressure and thereby reduce such noncompliance due to time saving. In addition, the programmable property of Blockchain can further prevent employees' noncompliance as rules and policy can be embedded into the Blockchain through the smart contacts and thereby their working tasks cannot be complete unless they meet certain security-procedure conditions.

On the other hand, when employees collude with external hackers to compromise the company's digital assets or commit such malicious deeds by themselves for personal monetary gains, they essentially act like external hackers with more privilege of accessing the company's digital assets. Such an insider data breach may be the most difficult one to thwart as this Trojan-horse employee is covered by his legitimate employee status. Fortunately, all aforementioned benefits of using Blockchain for preventing hacking can still apply to such insider data breaches. In addition, smart contracts can program certain employees to perform a given set of tasks, as employees' identity is known to the company and can be written into the smart contracts storing on the Blockchain network. For example, an employee is given the privilege to edit a newly

produced music. Although she/he has the access to copy/edit the music due to task requirement, she/he cannot obtain the ownership of this music as long as a smart contract is written to prevent such digital value transfer initiation. Accordingly, such employee cannot cash out the stolen music without appropriate ownership although she/he may be able to take advantage of this music personally. Therefore, combining the computational logic property of Blockchain technology with the *Least Privilege Principle*, a company can ensure that an employee is only able to perform the given tasks with tamper-resistant and predetermined privilege. Consequently, it is better off for an employee to obey the company's information security policy due to his bounded rationality and thereby greatly reduces the insider data breaches.

4.10. Concerns of Blockchain

As any other kinds of virtual currency, Bitcoin is challenging the traditional governmental control in our economic system. It reduces the profit of banks and indirectly of government if the banks are owned by the government. It increases the hardness of local government to trace its cash or money flows especially for the international transactions because all the blocks are encrypted and anonymous in the Blockchain in terms of owners' identities. Hence, it may promote the illegal trades, like drug or human traffic between nations.

In addition, Bitcoin can handle only seven transactions per second under its current network bandwidth allowance (BitcoinWiki 2017). As a comparison, the VISA network can process more than 2,000 transactions per second. The slow transaction speed may become an obstacle for Bitcoin being adopted widely.

Furthermore, its supporting infrastructure, Blockchain, is not immune to the worldwide natural disasters, especially those related to electronic power. Compared with the traditional paper note or gold, Bitcoin is not valuable when there is no power or a power shortage. Similarly, Blockchain can be infected by a worldwide computer virus as well. If some super-smart hackers could write such worldwide malicious codes and inject it into the Internet, the Blockchain will be the best tools for him to spread out virus, especially when the majority of computers have been infected. To illustrate, the another successful public Blockchain application, Ethereum, was hacked in 2016 for its DAO project due to a loophole in the programming code, although this is not the flaw of Blockchain mechanism (Vigna 2016). Hence, one needs to be caution about the risks involved in experimenting with Blockchain as its applications may still need some time to improve and perfect (Iansiti and Lakhani 2017).

4.11. Conclusions

This conceptual article aims to introduce the Blockchain technology and discuss how such profound technology can help to assist and advance information security. For decades, we have studied to build defense systems to prevent external hacking and enhance managerial policies to regulate employees' data breach. However, information security issues still remain as the top concerns in both practice and academy. The fundamental design of our old security models leaves the opportunities and incentives for hackers and insiders to breach the information assets of a company. We made lots of progress to prevent intruders from breaking into the systems and accessing valuable information, like "*Defense in Depth*" and data encryptions, but it also leaves a big blank after intruders have successfully hacked into the systems and gained a control of it. The fundamental idea behind it is based on the trusted third party (e.g.,

government, bank, corporation) to centralize control of our information assets because we believe they will have enough means to secure our data. However, with the advanced information technology, a certain intruder or a certain group of intruders sooner or later will outperform those trusted third party to seek their own self-interests and harm the rest of the public. The design of Blockchain has recognized the disadvantage of being controlled centrally (i.e., central point of failure), and hence, it creates a distributed ledger, which spreads across multiple sites, countries or institutions, and is typically public in the sense that anyone can view and audit it. Everything that we own and everything that we do is governed by those big piles of records in the Blockchain instead of a central trusted entity. Such radical design of Blockchain is controversial, disruptive, and breakthrough, but it is affecting a number of businesses to rethink their business models in the near future markets, especially the financial industry (Gupta and Knight 2017).

Furthermore, relying on the theory of bounded rationality, this paper sheds light on how the application of Blockchain can complement and improve current information security defense models. The information security research has switched from defending the products of hackers (e.g., computer virus) to hackers themselves, as destroy the leader and the gang will collapse. Such new focus leads information security companies (e.g., McAfee) to develop new defending systems to delay, trace, and identify hackers. With the help of local law enforcement, information security has been greatly improved. However, with the rapid development of new emerging technology (e.g., the Internet of Things), more and more international hackings and insider data breaches occur in the recent years. It seems that the focus on catching intruders is no longer the most effective strategy, as they become more difficult to identify and harder to

prosecute by law. Instead, we may need to defeat a hacker's mind as one's intention leads to his actual behavior according to the Theory of Planned Behavior (Ajzen 1991). If a certain mechanism can effectively undermine hackers' motivations for attack, hackers would have no incentives to commit the malicious deeds any more. Humans are limited for the cognitive capacity of their minds and the time available for them to make the most optimal decision; thus, they often make a good enough practical decision under their bounded rational. Through our illustrations in the paper, Blockchain is very suitable to support current information security models to dramatically increase the level of complexity of compromising information assets. Therefore, due to intruders' bounded rationality, applications of Blockchain with current countermeasures can greatly assist and advance information security.

CHAPTER 5. CONCLUSIONS

The central theme of this dissertation is about information security and compliance. This dissertation consists of three essays where each essay investigates the different aspects of information security, and it is aimed to address the growing concern of securing a company's information assets.

The first essay constructed a game theoretical model to study the diversity in a hacker's intrusion behaviors and the firm's costs to investigate the abnormal activities. This research filled the gap of uniformed hacker's type in the existing literature and provided insights to explain the phenomenon of the increasing number of hackings, especially *international* cyberattacks. It captured the natural interplay between a firm's investigations and a hacker's intrusions as a "cat and mouse" game; most importantly, it demonstrated that *international* hacking cannot be fully prevented, no matter what strategy a firm adopts as long as the cost of investigating data breaches exists. This information provides some managerial insights for a firm to strategically allocate its resources to prevent inevitable intrusions and could improve the firm's profits by treating security investments like costly insurance. In addition, this study showed that the specific percentage of hackers who can be deterred under a certain level of heavy punishment. In order to increase such a deterred percentage, firms are advised to continuously reduce monitoring cost and increase the precision of automated detection to minimize manual detection cost. Lastly, this study can guide a firm to dynamically learn from its surrounding cyber-environment to incorporate the external signals (e.g., a newspaper report or other media channels) with its own historical data to better defend its information assets.

The second essay conducted a series of laboratory experiments to explore the other side of information security data breaches caused by insiders' (e.g., employee) malicious deeds or noncompliance with information security policy. This research aimed to design a realistic incentive structure to help a company to better protect its information assets. It found that individual reward and punishment together with certainty is the best strategy for a company to regulate its employees' noncompliance. This finding suggests that, in the long run, a company shall always employ both means to achieve better regulating power, although it may cost the company some capital for rewarding. Additionally, individual reward is always better than individual punishment for intensifying information security policy compliance. It demonstrated that employee's perception of security procedure is not in line with the company's, as the employee wants more work done but the company wants more work done securely. Modern fast-pace life style may make employees pursue more self-interests and short-run benefits. Hence, giving a reward for compliant behavior can align both parties' interests. Furthermore, the superior complementary effect between reward and punishment was always observed no matter in individual form or collective form. Lastly, a company is also advised to avoid hiring risk-loving, impulsive, and junior people (if possible) for the key positions which hold its critical information assets. This is because those employees may pose a stronger threat to a company's security defense and their compliance may not be easily improved by rewards or/and punishments no matter in what forms.

After understanding both sides of information security, external hackers' hacking behaviors as well as internal insiders' noncompliance, the third essay introduced Blockchain

technology and discussed how such profound technology can help to prevent information breaches. Instead of the old security models that store valuable information in the servers of trusted third parties, the design of Blockchain has recognized the disadvantage of being controlled centrally (i.e., central point of failure), and hence, it creates a distributed ledger, which spreads across multiple sites, countries or institutions, and is typically public in the sense that anyone can view and audit it. This article also discussed the new transition that defeating intruders' motivation of hacking can lead to their less malicious deeds. Moreover, relying on the Theory of Bounded Rationality, this study illustrated how Blockchain technology can dramatically increase the level of complexity of compromising information assets and meanwhile undermine intruders' motivation of monetary gains. Accordingly, companies are advised to explore such breakthrough technology, Blockchain, with current information security countermeasures to better protect their information assets.

REFERENCES

Abrams, R. 2014. "Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop," in: *The New York Times*.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational behavior and human decision processes* (50:2), pp. 179-211.

Alaskar, M., Vodanovich, S., and Shen, K. N. 2015. "Evolvement of Information Security Research on Employees' Behavior: A Systematic Review and Future Direction," *System Sciences (HICSS), 2015 48th Hawaii International Conference on*: IEEE, pp. 4241-4250.

Alexander, C. S., and Becker, H. J. 1978. "The Use of Vignettes in Survey Research," *Public opinion quarterly* (42:1), pp. 93-104.

Alpcan, T., and Basar, T. 2006. "An Intrusion Detection Game with Limited Observations," *Proceedings of the 12th Int. Symp. on Dynamic Games and Applications*.

Anderson, D., Frivold, T., and Valdes, A. 1995. "Next-Generation Intrusion Detection Expert System (Nides): A Summary."

Andreoni, J., Harbaugh, W., and Vesterlund, L. 2003. "The Carrot or the Stick: Rewards, Punishments, and Cooperation," *The American Economic Review* (93:3), pp. 893-902.

Balliet, D., Mulder, L. B., and Van Lange, P. A. 2011. "Reward, Punishment, and Cooperation: A Meta-Analysis," *Psychological bulletin* (137:4), p. 594.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce It Policy Violation," *Computers & security* (39), pp. 145-159.

Becker, C. 1968. "Punishment: An Economic Approach, 76j," *Pol. Econ* (169:10.2307), p. 1830482169.

Becker, G. S. 1974. "Crime and Punishment: An Economic Approach," in *Essays in the Economics of Crime and Punishment*. NBER, pp. 1-54.

Bertsekas, D. P., Bertsekas, D. P., Bertsekas, D. P., and Bertsekas, D. P. 1995. *Dynamic Programming and Optimal Control*. Athena Scientific Belmont, MA.

Bisson, D. 2013. "Five Hackers Added to Fbi's Cyber Most Wanted List," in: *The State of Security*.

BitcoinWiki. 2017. "Scalability." from https://en.bitcoin.it/wiki/Scalability

Bloem, M., Alpcan, T., and Basar, T. 2006. "Intrusion Response as a Resource Allocation Problem," *Decision and Control, 2006 45th IEEE Conference on*: IEEE, pp. 6283-6288.

Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., and Wustrow, E. 2014. "Elliptic Curve Cryptography in Practice," *International Conference on Financial Cryptography and Data Security*: Springer, pp. 157-175.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18:2), pp. 151-164.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2009. "Effects of Individual and Organization Based Beliefs and the Moderating Role of Work Experience on Insiders' Good Security Behaviors," *Computational Science and Engineering, 2009. CSE'09. International Conference on*: IEEE, pp. 476-481.

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

Çakanyıldırım, M., Yue, W. T., and Ryu, Y. U. 2009. "The Management of Intrusion Detection: Configuration, Inspection, and Investment," *European Journal of Operational Research* (195:1), pp. 186-204.

Cao, L. 2004. *Major Criminological Theories: Concepts and Measurements*. Wadsworth/Thomson Learning.

Casey, M., and Wong, P. 2017. "Global Supply Chains Are About to Get Better, Thanks to Blockchain." Harvard Business Review.

Catalini, C. 2017. "How Blockchain Applications Will Move Beyond Finance." Harvard Business Review.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16:1), pp. 28-46.

Chang, S. E., and Ho, C. B. 2006. "Organizational Factors to the Effectiveness of Implementing Information Security Management," *Industrial Management & Data Systems* (106:3), pp. 345-361.

Chen, D. L., Schonger, M., and Wickens, C. 2016. "Otree—an Open-Source Platform for Laboratory, Online, and Field Experiments," *Journal of Behavioral and Experimental Finance* (9), pp. 88-97.

Chen, Y., Ramamurthy, K., and Wen, K.-W. 2012. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," *Journal of Management Information Systems* (29:3), pp. 157-188.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. 2013. "Understanding the Violation of Is Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory," *Computers & Security* (39), pp. 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), pp. 186-196.

Cornish, D. B., and Clarke, R. V. 1987. "Understanding Crime Displacement: An Application of Rational Choice Theory," *Criminology* (25:4), pp. 933-948.

Cremonini, M., and Nizovtsev, D. 2009. "Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers," *Journal of Management Information Systems* (26:3), pp. 241-274.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

D'Arcy, J., and Hovav, A. 2009. "Does One Size Fit All? Examining the Differential Effects of Is Security Countermeasures," *Journal of business ethics* (89:1), pp. 59-71.

Dallin, D. J., and Nicolaevsky, B. I. 1947. "Forced Labor in Soviet Russia."

Deloitte. 2015. "Blockchain Disrupting the Financial Services Industry?."

Dhillon, G., and Backhouse, J. 2000. "Technical Opinion: Information System Security Management in the New Millennium," *Communications of the ACM* (43:7), pp. 125-128.

Driscoll, S. 2013. "How Bitcoin Works under the Hood," in: *ImponderableThings*. Blogger.

Dutta, A., and McCrohan, K. 2002. "Management's Role in Information Security in a Cyber Economy," *California Management Review* (45:1), pp. 67-87.

Edney, J. J., and Harper, C. S. 1978. "The Commons Dilemma," *Environmental Management* (2:6), pp. 491-507.

Eisenhardt, K. M. 1989. "Agency Theory: An Assessment and Review," *Academy of management review* (14:1), pp. 57-74.

Ernst, and Young. 2008. "Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey."

Ernst, Y. L., and Young, X. 2002. "Global Information Security Survey," *UK: Presentation Services*.

Estonian. 2017. "Digital Society - E-Estonia." from https://e-estonia.com/the-story/digital-society/

Eyal, I., Gencer, A. E., Sirer, E. G., and Van Renesse, R. 2016. "Bitcoin-Ng: A Scalable Blockchain Protocol," *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pp. 45-59.

Fehr, E., and Fischbacher, U. 2003. "The Nature of Human Altruism," *Nature* (425:6960), pp. 785-791.

Fehr, E., and Gächter, S. 1999. "Cooperation and Punishment in Public Goods Experiments," *Institute for Empirical Research in Economics working paper*:10.

Fehr, E., and Gächter, S. 2000. "Cooperation and Punishment in Public Goods Experiments," *American Economic Review* (90:4), pp. 980-994.

Finne, T. 2000. "Information Systems Risk Management: Key Concepts and Business Processes," *Computers & Security* (19:3), pp. 234-242.

Fudenberg, D., and Tirole, J. 1991. "Game Theory," *Cambridge, Massachusetts* (393).

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., and Vázquez, E. 2009. "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," *computers & security* (28:1), pp. 18-28.

Gigerenzer, G., and Selten, R. 2002. *Bounded Rationality: The Adaptive Toolbox*. MIT press.

Gilham, S. A. 1994. "The Marines Build Men: Resocialization and Recruit Training," *THE SOCIOLOGICAL OUTLOOK231* (239).

Glazer, E., and Yadron, D. 2014. "Jp Morgan Says About 76 Million Households Affected by Cyber Breach," *Wall Street Journal* (2).

Goel, V., and Perlroth, N. 2016. "Yahoo Says 1 Billion User Accounts Were Hacked," *New York Times, Dec* (14).

Granville, K. 2015. "9 Recent Cyberattacks against Big Businesses," in: *The New York Times*.

Guo, K. H., and Yuan, Y. 2012. "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model," *Information & management* (49:6), pp. 320-326.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems* (28:2), pp. 203-236.

Gupta, V., and Knight, R. 2017. "How Blockchain Could Help Emerging Markets Leap Ahead." Harvard Business Review.

Gürerk, Ö., Irlenbusch, B., and Rockenbach, B. 2006. "The Competitive Advantage of Sanctioning Institutions," *Science* (312:5770), pp. 108-111.

Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly*, pp. 257-278.

Hashim, M. J., and Bockstedt, J. C. 2015. "Overcoming Free-Riding in Information Goods: Sanctions or Rewards?," *System Sciences (HICSS), 2015 48th Hawaii International Conference on*: IEEE, pp. 4834-4843.

Heckathorn, D. D. 1988. "Collective Sanctions and the Creation of Prisoner's Dilemma Norms," *American Journal of Sociology*, pp. 535-562.

Heckathorn, D. D. 1990. "Collective Sanctions and Compliance Norms: A Formal Theory of Group-Mediated Social Control," *American Sociological Review*, pp. 366-384.

Henrich, J. 2006. "Cooperation, Punishment, and the Evolution of Human Institutions," *Science(Washington)* (311:5769), pp. 60-61.

Herath, T., and Rao, H. R. 2009a. "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems* (47:2), pp. 154-165.

Herath, T., and Rao, H. R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Holt, C. A., and Laury, S. K. 2002. "Risk Aversion and Incentive Effects," *American economic review* (92:5), pp. 1644-1655.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. 2012. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*," *Decision Sciences* (43:4), pp. 615-660.

Hu, Q., West, R., and 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), pp. 6-48.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?," *Communications of the ACM* (54:6), pp. 54-60.

Iansiti, M., and Lakhani, K. R. 2017. "The Truth About Blockchain," *Harvard Business Review* (95:1), pp. 118-127.

Ilgun, K., Kemmerer, R. A., and Porras, P. A. 1995. "State Transition Analysis: A Rule-Based Intrusion Detection Approach," *IEEE transactions on software engineering* (21:3), pp. 181-199.

Khan, L., Awad, M., and Thuraisingham, B. 2007. "A New Intrusion Detection System Using Support Vector Machines and Hierarchical Clustering," *The VLDB Journal—The International Journal on Very Large Data Bases* (16:4), pp. 507-521.

Kollock, P. 1998. "Social Dilemmas: The Anatomy of Cooperation," *Annual review of sociology*, pp. 183-214.

Kroll. 2016. "Global Fraud & Risk Report: Building Resilience in a Volatile World."

Krumpal, I. 2013. "Determinants of Social Desirability Bias in Sensitive Surveys: A Literature Review," *Quality & Quantity* (47:4), pp. 2025-2047.

Kumar, S., and Spafford, E. H. 1995. "A Software Architecture to Support Misuse Intrusion Detection."

Lee, S. M., Lee, S.-G., and Yoo, S. 2004. "An Integrative Model of Computer Abuse Based on Social Control and General Deterrence Theories," *Information & Management* (41:6), pp. 707-718.

Lee, W., and Stolfo, S. J. 2000. "A Framework for Constructing Features and Models for Intrusion Detection Systems," *ACM transactions on Information and system security (TiSSEC)* (3:4), pp. 227-261.

Liang, H., Xue, Y., and Wu, L. 2013. "Ensuring Employees' It Compliance: Carrot or Stick?," *Information Systems Research* (24:2), pp. 279-294.

Lin, J.-C., Chen, J.-M., Chen, C.-C., and Chien, Y.-S. 2009. "A Game Theoretic Approach to Decision and Analysis in Strategies of Attack and Defense," *Secure Software Integration and Reliability Improvement, 2009. SSIRI 2009. Third IEEE International Conference on*: IEEE, pp. 75-81.

Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., and Das, K. 2000. "The 1999 Darpa Off-Line Intrusion Detection Evaluation," *Computer networks* (34:4), pp. 579-595.

Liu, Y., Comaniciu, C., and Man, H. 2006. "A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks," *Proceeding from the 2006 workshop on Game theory for communications and networks*: ACM, p. 4.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, pp. 173-186.

Locke, J., Yolton, J. W., and Yolton, J. S. 1989. *The Clarendon Edition of the Works of John Locke: Some Thoughts Concerning Education*. Clarendon Press.

Lynn, M., and Oldenquist, A. 1986. "Egoistic and Nonegoistic Motives in Social Dilemmas," *American Psychologist* (41:5), p. 529.

Mathews, A., and Yadron, D. 2015. "Health Insurer Anthem Hit by Hackers."

Mathews, A. W. 2015. "Anthem: Hacked Database Included 78.8 Million People," *Wall Street Journal* (24).

McCue, A. 2008. "Beware the Insider Security Threat," *CIO Jury*.

McFarland, C., Paget, F., and Samani, R. 2015. "The Hidden Data Economy," McAfee Labs, McAfee. Part of Intel Security.

McKendrick, J. 2016. "Disney, Yes Disney, Becomes Blockchain's Biggest Proponent | Zdnet."

Mitnick, K. D., and Simon, W. L. 2001. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

Mueller-Eberstein, M. 2017. "The Next Radical Internet Transformation: How Blockchain Technology Is Transforming Business, Governments, Computing, and Security Models."

Murck, P. 2017. "Who Controls the Blockchain?", from https://hbr.org/2017/04/who-controls-the-blockchain

Muth, J. F. 1961. "Rational Expectations and the Theory of Price Movements," *Econometrica: Journal of the Econometric Society*, pp. 315-335.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules&Quest; an Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."

Nguyen, K. C., Alpcan, T., and Basar, T. 2009. "Security Games with Incomplete Information," *Communications, 2009. ICC'09. IEEE International Conference on*: IEEE, pp. 1-6.

Osborne, M. J., and Rubinstein, A. 1994. *A Course in Game Theory*. MIT press.

Ostrom, E., Walker, J., and Gardner, R. 1992. "Covenants with and without a Sword: Self-Governance Is Possible," *American political science Review* (86:02), pp. 404-417.

Padayachee, K. 2012. "Taxonomy of Compliant Information Security Behavior," *Computers & Security* (31:5), pp. 673-680.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on*: IEEE, pp. 156b-156b.

Patcha, A., and Park, J.-M. 2004. "A Game Theoretic Approach to Modeling Intrusion Detection in Mobile Ad Hoc Networks," *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*: IEEE, pp. 280-284.

Peck, M. 2015. "The Future of the Web Looks a Lot Like Bitcoin," *Spectrum IEEE (1 July)*.

Peretti, K. K. 2008. "Data Breaches: What the Underground World of Carding Reveals," *Santa Clara Computer & High Tech. LJ* (25), p. 375.

Perlroth, N., Airbnb, R., and Etsy, S. 2016. "Hackers Used New Weapons to Disrupt Major Websites across Us," *New York Times* (21).

Pogarsky, G. 2004. "Projected Offending and Contemporaneous Rule-Violation: Implications for Heterotypic Continuity*," *Criminology* (42:1), pp. 111-136.

Popper, N. 2015. "Bitcoin Technology Piques Interest on Wall St," *The New York Times*.

Popper, N. 2016a. "Central Banks Consider Bitcoin's Technology, If Not Bitcoin," in: *The New York Times*.

Popper, N. 2016b. "Ethereum, a Virtual Currency," *Enables Transactions That Rival Bitcoin's. The New York Times. Retrieved from* http://www.*nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html*.

Popper, N. 2017. "What Is Bitcoin? All About the Mysterious Digital Currency," in: *The New York Times*.

Porras, P. A., and Neumann, P. G. 1997. "Emerald: Event Monitoring Enabling Response to Anomalous Live Disturbances," *Proceedings of the 20th national information systems security conference*, pp. 353-365.

PricewaterhouseCoopers. 2008. "Employee Behaviour Key to Improving Information Security, New Survey Finds."

Puhakainen, P., and Ahonen, R. 2006. "Design Theory for Information Security Awareness."

PwC. 2015. "Information Security Breaches Survey."

Rand, D. G., Dreber, A., Ellingsen, T., Fudenberg, D., and Nowak, M. A. 2009. "Positive Interactions Promote Public Cooperation," *Science* (325:5945), pp. 1272-1275.

Richardson, R., and Director, C. 2008. "Csi Computer Crime and Security Survey," *Computer Security Institute* (1), pp. 1-30.

Rockefeller, S. 2014. "A Kill Chain Analysis of the 2013 Target Data Breach," tech. rep., Committee on Commerce, Science and Transportation.

Sanger, D., and Perlroth, N. 2015. "Bank Hackers Steal Millions Via Malware," in: *The New York Times*.

Sanger, D., Schmidt, M., and Perlroth, N. 2014. "Obama Vows a Response to Cyberattack on Sony," in: *The New York Times*.

Sanger, D. E., and Savage, C. 2016. "Us Says Russia Directed Hacks to Influence Elections," *New York Times*.

Schmidt, M., and Sanger, D. 2015. "Russian Hackers Read Obama's Unclassified Emails, Officials Say," in: *The New York Times*.

Scott, M. 2014. "Estonians Embrace Life in a Digital World," in: *The New York Times*.

Secretary, O. o. t. P. 2015. "Securing Cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts." The White House.

Sequeira, K., and Zaki, M. 2002. "Admit: Anomaly-Based Data Mining for Intrusions," *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*: ACM, pp. 386-395.

Sigmund, K. 2007. "Punish or Perish? Retaliation and Collaboration among Humans," *Trends in ecology & evolution* (22:11), pp. 593-600.

Simon, H. A. 1955. "A Behavioral Model of Rational Choice," *The quarterly journal of economics* (69:1), pp. 99-118.

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2).

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), p. 487.

So, M. W., and Sculli, D. 2002. "The Role of Trust, Quality, Value and Risk in Conducting E-Business," *Industrial Management & Data Systems* (102:9), pp. 503-512.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security* (22:1), pp. 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), pp. 296-302.

Stolfo, S. J., Lee, W., Chan, P. K., Fan, W., and Eskin, E. 2001. "Data Mining-Based Intrusion Detectors: An Overview of the Columbia Ids Project," *ACM SIGMOD Record* (30:4), pp. 5-14.

Straub Jr, D. W. 1990. "Effective Is Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Straub Jr, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly*, pp. 45-60.

Tapscott, D., and Tapscott, A. 2016. "The Impact of the Blockchain Goes Beyond Financial Services," *Harvard Business Review*.

Thomson, I. 2007. "Hmrc Data Loss Leaves 25 Million Exposed," in: *ITN News*.

Trevino, L. K. 1992. "Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations," *Business Ethics Quarterly* (2:02), pp. 121-136.

Tversky, A., and Kahneman, D. 1986. "Rational Choice and the Framing of Decisions," *Journal of business*, pp. S251-S278.

US-CERT. 2009. "United States Computer Emergency Readiness Team." from https://www.us-cert.gov/

van den Hoven, J. 1999. "Management: Stewards of Data."

Van Lange, P. A., and Joireman, J. A. 2008. "How We Can Promote Behavior That Serves All of Us in the Future," *Social Issues and Policy Review* (2:1), pp. 127-157.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3), pp. 190-198.

Vance, A., and Siponen, M. T. 2012. "Is Security Policy Violations: A Rational Choice Perspective," *Journal of Organizational and End User Computing (JOEUC)* (24:1), pp. 21-41.

Vermeulen, C., and Von Solms, R. 2002. "The Information Security Management Toolbox–Taking the Pain out of Security Management," *Information Management & Computer Security* (10:3), pp. 119-125.

Vigna, P. 2016. "Cryptocurrency Platform Ethereum Gets a Controversial Update." The Wall Street Journal.

Von Solms, B., and Von Solms, R. 2004. "The 10 Deadly Sins of Information Security Management," *Computers & Security* (23:5), pp. 371-376.

Wallace, G. 2014. "Hvac Vendor Eyed as Entry Point for Target Breach," in: *CNN Money*.

Walport, M. 2016. "Distributed Ledger Technology: Beyond Blockchain," *UK Government Office for Science, Tech. Rep* (19).

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), p. 101.

Wueest, C. 2015. "Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services." from http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

Yamagishi, T. 1986. "The Provision of a Sanctioning System as a Public Good," *Journal of Personality and social Psychology* (51:1), p. 110.

Yamagishi, T. 1988. "Seriousness of Social Dilemmas and the Provision of a Sanctioning System," *Social Psychology Quarterly*, pp. 32-42.

Yu, H., Yang, J., and Han, J. 2003. "Classifying Large Data Sets Using Svms with Hierarchical Clusters," *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*: ACM, pp. 306-315.

Zhao, F. 2004. "Management of Information Technology and Business Process Re-Engineering: A Case Study," *Industrial Management & Data Systems* (104:8), pp. 674-680.

APPENDIX A. 30 SCENARIOS FOR INFORMATION SECURITY POLICY VIOLATIONS

Scenario # [unknown to participants]	Severity (token worth) [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 et al. (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 Experiment 1-4

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

Experiment 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".

Experiment 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".

Experiment 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.

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

APPENDIX F. SUMMARY OF KEY NOTATIONS

Notation	Description
θ_H	Hacker's type
S_H	Hacker's strategy space
S_F	Firm's strategy space
s_H	Hacker's strategy action
s_F	Firm's strategy action
U_H	Hacker's payoff
U_F	Firm's payoff
c	Cost of monitoring intrusion behaviors
c^D	Cost of investigating a *domestic* hacker including monitor cost
c^I	Cost of investigating an *international* hacker including monitor cost
d	The damage of firm by an uninvestigated intrusion
ϕ	Fraction of damage recovered by an investigation process
μ	Benefit of hacker for intrusions
β^D	Expected penalty of a *domestic* hacker for intrusions
β^I	Expected penalty of an *international* hacker for intrusions
q	Prior of firm to believe that hacker is *domestic*
$w(\theta_H)$	Cost of investigating hacker θ_H including monitor cost
$g(\theta_H)$	Expected penalty of hacker θ_H for intrusions
$\bar{\theta}_H$	Marginal hacker who is indifferent between NOT hacking and hacking
$f(\theta_H)$	Probability density function over hacker's type θ_H
τ_i	The time point of the i^{th} simultaneous game
q_i	Belief of firm that hacker is *domestic* in the i^{th} game
ε_i	External signal, indicating the strength/frequency of domestic hacking over all intrusions during time period (τ_i, τ_{i+1})

APPENDIX G. IRB APPROVAL LETTERS AND CONSENT FORM

IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Institutional Review Board
Office for Responsible Research
Vice President for Research
1138 Pearson Hall
Ames, Iowa 50011-2207
515 294-4566
FAX 515 294-4267

Date: 3/22/2016

To: Yuanxiang Li
3128 Gerdin Business Building

CC: Dr. Elizabeth Hoffman
367 Heady Hall

From: Office for Responsible Research

Title: Information Security and Decision Making

IRB ID: 16-086

Approval Date:	3/22/2016	**Date for Continuing Review:**	3/21/2018
Submission Type:	New	**Review Type:**	Expedited

The project referenced above has received approval from the Institutional Review Board (IRB) at Iowa State University according to the dates shown above. Please refer to the IRB ID number shown above in all correspondence regarding this study.

To ensure compliance with federal regulations (45 CFR 46 & 21 CFR 56), please be sure to:

Use only the approved study materials in your research, **including the recruitment materials and informed consent documents that have the IRB approval stamp**.

Retain signed informed consent documents for 3 years after the close of the study, when documented consent is required.

Obtain IRB approval prior to implementing any changes to the study by submitting a Modification Form for Non-Exempt Research or Amendment for Personnel Changes form, as necessary.

Immediately inform the IRB of (1) all serious and/or unexpected adverse experiences involving risks to subjects or others; and (2) **any other unanticipated problems involving risks** to subjects or others.

Stop all research activity if IRB approval lapses, unless continuation is necessary to prevent harm to research participants. Research activity can resume once IRB approval is reestablished.

Complete a new continuing review form at least three to four weeks prior to the **date for continuing review** as noted above to provide sufficient time for the IRB to review and approve continuation of the study. We will send a courtesy reminder as this date approaches.

Please be aware that IRB approval means that you have met the requirements of federal regulations and ISU policies governing human subjects research. **Approval from other entities may also be needed.** For example, access to data from private records (e.g. student, medical, or employment records, etc.) that are protected by FERPA, HIPAA, or other confidentiality policies requires permission from the holders of those records. Similarly, for research conducted in institutions other than ISU (e.g., schools, other colleges or universities, medical facilities, companies, etc.), investigators must obtain permission from the institution(s) as required by their policies. **IRB approval in no way implies or guarantees that permission from these other entities will be granted.**

Upon completion of the project, please submit a Project Closure Form to the Office for Responsible Research, 1138 Pearson Hall, to officially close the project.

Please don't hesitate to contact us if you have questions or concerns at 515-294-4566 or IRB@iastate.edu.

IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Institutional Review Board
Office for Responsible Research
Vice President for Research
2420 Lincoln Way, Suite 202
Ames, Iowa 50014
515 294-4566

Date: 9/7/2016

To: Yuanxiang Li
3128 Gerdin Business Building

CC: Dr. Elizabeth Hoffman
367 Heady Hall

From: Office for Responsible Research

Title: Information Security and Decision Making

IRB ID: 16-086

Approval Date:	9/7/2016	**Date for Continuing Review:**	3/21/2018
Submission Type:	Modification	**Review Type:**	Expedited

The project referenced above has received approval from the Institutional Review Board (IRB) at Iowa State University according to the dates shown above. Please refer to the IRB ID number shown above in all correspondence regarding this study.

To ensure compliance with federal regulations (45 CFR 46 & 21 CFR 56), please be sure to:

- **Use only the approved study materials** in your research, **including the recruitment materials and informed consent documents that have the IRB approval stamp**.
- **Retain signed informed consent documents for 3 years after the close of the study,** when documented consent is required.
- **Obtain IRB approval prior to implementing any changes** to the study by submitting a Modification Form for Non-Exempt Research or Amendment for Personnel Changes form, as necessary.
- **Immediately inform the IRB of** (1) **all serious and/or unexpected adverse experiences** involving risks to subjects or others; and (2) **any other unanticipated problems involving risks** to subjects or others.
- **Stop all research activity if IRB approval lapses**, unless continuation is necessary to prevent harm to research participants. Research activity can resume once IRB approval is reestablished.
- **Complete a new continuing review form** at least three to four weeks prior to the **date for continuing review** as noted above to provide sufficient time for the IRB to review and approve continuation of the study. We will send a courtesy reminder as this date approaches.

Please be aware that IRB approval means that you have met the requirements of federal regulations and ISU policies governing human subjects research. **Approval from other entities may also be needed.** For example, access to data from private records (e.g. student, medical, or employment records, etc.) that are protected by FERPA, HIPAA, or other confidentiality policies requires permission from the holders of those records. Similarly, for research conducted in institutions other than ISU (e.g., schools, other colleges or universities, medical facilities, companies, etc.), investigators must obtain permission from the institution(s) as required by their policies. **IRB approval in no way implies or guarantees that permission from these other entities will be granted.**

Upon completion of the project, please submit a Project Closure Form to the Office for Responsible Research, 202 Kingland, to officially close the project.

Please don't hesitate to contact us if you have questions or concerns at 515-294-4566 or IRB@iastate.edu.

IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Institutional Review Board
Office for Responsible Research
Vice President for Research
2420 Lincoln Way, Suite 202
Ames, Iowa 50014
515 294-4566

Date: 9/26/2016

To: Yuanxiang Li
3128 Gerdin Business Building

CC: Dr. Elizabeth Hoffman
367 Heady Hall

From: Office for Responsible Research

Title: Information Security and Decision Making

IRB ID: 16-086

Approval Date:	9/26/2016	**Date for Continuing Review:**	3/21/2018
Submission Type:	Modification	**Review Type:**	Expedited

The project referenced above has received approval from the Institutional Review Board (IRB) at Iowa State University according to the dates shown above. Please refer to the IRB ID number shown above in all correspondence regarding this study.

To ensure compliance with federal regulations (45 CFR 46 & 21 CFR 56), please be sure to:

- **Use only the approved study materials** in your research, **including the recruitment materials and informed consent documents that have the IRB approval stamp**.
- **Retain signed informed consent documents for 3 years after the close of the study**, when documented consent is required.
- **Obtain IRB approval prior to implementing any changes** to the study by submitting a Modification Form for Non-Exempt Research or Amendment for Personnel Changes form, as necessary.
- **Immediately inform the IRB of** (1) **all serious and/or unexpected adverse experiences** involving risks to subjects or others; and (2) **any other unanticipated problems involving risks** to subjects or others.
- **Stop all research activity if IRB approval lapses**, unless continuation is necessary to prevent harm to research participants. Research activity can resume once IRB approval is reestablished.
- **Complete a new continuing review form** at least three to four weeks prior to the **date for continuing review** as noted above to provide sufficient time for the IRB to review and approve continuation of the study. We will send a courtesy reminder as this date approaches.

Please be aware that IRB approval means that you have met the requirements of federal regulations and ISU policies governing human subjects research. **Approval from other entities may also be needed.** For example, access to data from private records (e.g. student, medical, or employment records, etc.) that are protected by FERPA, HIPAA, or other confidentiality policies requires permission from the holders of those records. Similarly, for research conducted in institutions other than ISU (e.g., schools, other colleges or universities, medical facilities, companies, etc.), investigators must obtain permission from the institution(s) as required by their policies. **IRB approval in no way implies or guarantees that permission from these other entities will be granted.**

Upon completion of the project, please submit a Project Closure Form to the Office for Responsible Research, 202 Kingland, to officially close the project.

Please don't hesitate to contact us if you have questions or concerns at 515-294-4566 or IRB@iastate.edu.

ISU IRB # 1 16-086
Approved Date: 22 March 2016
Expiration Date: 21 March 2018

For Non-SONA System

INFORMED CONSENT DOCUMENT

Title of Study: Information Security and Decision Making

Investigators: Yuanxiang John Li, Dr. Elizabeth Hoffman, and Dr. Dan Zhu

This form describes a research project. It has information to help you decide whether or not you wish to participate. Research studies include only people who choose to take part—your participation is completely voluntary. Please discuss any questions you have about the study or about this form with the project staff before deciding to participate.

Introduction

The purpose of this study is to obtain a greater understanding of how a company's managerial policy will influence its employees' decision making on the information security policy. You are being invited to participate in this study because you showed an interest in the study. You should not participate if you are under age of 18.

Description of Procedures

If you agree to participate, you will be asked to come to a computer lab at the College of Business or the Department of Economics. You will play the role of Josh who is an employee of a company and answer some scenario-based questions on the behalf of Josh. Then you will fill demographic characteristics. Your participation will last for about 45 minutes.

Risks or Discomforts

There are no foreseeable risks at this time in participating in the study.

Benefits

If you decide to participate in this study, there is no direct benefit to you. It is hoped that the information gained in this study will benefit society by providing more insight to a company to better secure its information assets.

Costs and Compensation

You will not have any costs from participating in this study. A $5 show-up fee will be given to you in thanks for your participation. You will be compensated $10 on average for participating in this study. Your compensation may vary depending on your decision made on study tasks. You will need to complete a form to receive payment.

Participant Rights

Participating in this study is completely voluntary. You may choose not to take part in the study or to stop participating at any time, for any reason, without penalty or negative consequences. You can skip any questions that you do not wish to answer. If you have any questions *about the rights of research subjects or research-related injury*, please contact the IRB Administrator, (515) 294-4566, IRB@iastate.edu, or Director, (515) 294-3115, Office for Responsible Research, Iowa State University, Ames, Iowa 50011.

ISU IRB # 1 16-086
Approved Date: 22 March 2016
Expiration Date: 21 March 2018

For Non-SONA System

Confidentiality

Records identifying participants will be kept confidential to the extent permitted by applicable laws and regulations and will not be made publicly available. However, federal government regulatory agencies, auditing departments of Iowa State University, and the Institutional Review Board (a committee that reviews and approves human subject research studies) may inspect and/or copy study records for quality assurance and data analysis. These records may contain private information.

To ensure confidentiality to the extent permitted by law, the following measures will be taken: All research data will be stored securely and confidentially in locked cabinets. All identifiable information about you will be removed from your data with only a code to identify you. The codes that link your name to the data will be kept separate from the study data. Participant names will not be published. All electronic data will be stored on a secure network server, or on portable devices, such as a laptop, with encryption software and password protection.

Questions

You are encouraged to ask questions at any time during this study. For further information ***about the study,*** contact Yuanxiang John Li, 3128 Gerdin Business Building, yxli@iastate.edu; or Dr. Elizabeth Hoffman at bhoffman@iastate.edu.

Consent and Authorization Provisions

Your signature indicates that you voluntarily agree to participate in this study, that the study has been explained to you, that you have been given the time to read the document, and that your questions have been satisfactorily answered. You will receive a copy of the written informed consent prior to your participation in the study.

Participant's Name (printed) _____

_____ _____

Participant's Signature Date

ISU IRB # 1 16-086
Approved Date: 22 March 2016
Expiration Date: 21 March 2018

For SONA System

INFORMED CONSENT DOCUMENT

Title of Study: Information Security and Decision Making

Investigators: Yuanxiang John Li, Dr. Elizabeth Hoffman, and Dr. Dan Zhu

This form describes a research project. It has information to help you decide whether or not you wish to participate. Research studies include only people who choose to take part—your participation is completely voluntary. Please discuss any questions you have about the study or about this form with the project staff before deciding to participate.

Introduction

The purpose of this study is to obtain a greater understanding of how a company's managerial policy will influence its employees' decision making on the information security policy. You are being invited to participate in this study because you showed an interest in the study. You should not participate if you are under age of 18.

Description of Procedures

If you agree to participate, you will be asked to come to a computer lab at the College of Business or the Department of Economics. You will play the role of Josh who is an employee of a company and answer some scenario-based questions on the behalf of Josh. Then you will fill demographic characteristics. Your participation will last for about 45 minutes.

Risks or Discomforts

There are no foreseeable risks at this time in participating in the study.

Benefits

If you decide to participate in this study, there is no direct benefit to you. It is hoped that the information gained in this study will benefit society by providing more insight to a company to better secure its information assets.

Costs and Compensation

You will not have any costs from participating in this study. One course credit will be given to you in thanks for your participation toward your course grade in Marketing 340. If you are not able to participate in this study, alternative ways to earn the equivalent credit are listed in your MKT 340 course syllabus. You will be compensated $10 on average for participating in this study. Your compensation may vary depending on your decision made on study tasks. You will need to complete a form to receive payment.

Participant Rights

Participating in this study is completely voluntary. You may choose not to take part in the study or to stop participating at any time, for any reason, without penalty or negative consequences. You can skip any questions that you do not wish to answer. If you have any questions *about the rights of research subjects or research-related injury*, please contact the IRB Administrator,

ISU IRB # 1 16-086
Approved Date: 22 March 2016
Expiration Date: 21 March 2018

For SONA System

(515) 294-4566, IRB@iastate.edu, or Director, (515) 294-3115, Office for Responsible Research, Iowa State University, Ames, Iowa 50011.

Confidentiality

Records identifying participants will be kept confidential to the extent permitted by applicable laws and regulations and will not be made publicly available. However, federal government regulatory agencies, auditing departments of Iowa State University, and the Institutional Review Board (a committee that reviews and approves human subject research studies) may inspect and/or copy study records for quality assurance and data analysis. These records may contain private information.

To ensure confidentiality to the extent permitted by law, the following measures will be taken: All research data will be stored securely and confidentially in locked cabinets. All identifiable information about you will be removed from your data with only a code to identify you. The codes that link your name to the data will be kept separate from the study data. Participant names will not be published. All electronic data will be stored on a secure network server, or on portable devices, such as a laptop, with encryption software and password protection.

Questions

You are encouraged to ask questions at any time during this study. For further information ***about the study,*** contact Yuanxiang John Li, 3128 Gerdin Business Building, yxli@iastate.edu; or Dr. Elizabeth Hoffman at bhoffman@iastate.edu.

Consent and Authorization Provisions

Your signature indicates that you voluntarily agree to participate in this study, that the study has been explained to you, that you have been given the time to read the document, and that your questions have been satisfactorily answered. You will receive a copy of the written informed consent prior to your participation in the study.

Participant's Name (printed) _____

_____ _____

Participant's Signature Date