INTERNATIONAL JOURNAL OF HUMAN–COMPUTER INTERACTION
2016, VOL. 32, NO. 7, 557–567
http://dx.doi.org/10.1080/10447318.2016.1183862

Nontechnical Deterrence Effects of Mild and Severe Internet Use Policy Reminders in Reducing Employee Internet Abuse

Morgan M. Shepherd[a] and Roberto J. Mejias[b]

[a]College of Business, University of Colorado–Colorado Springs, Colorado Springs, Colorado, USA; [b]Hasan School of Business and Colorado State University–Pueblo, Pueblo, Colorado, USA

ABSTRACT
This two-stage longitudinal study examines how employee Internet abuse may be reduced by nontechnical deterrence methods, specifically via organizational acceptable use policies (AUPs). This study used actual employee usage and audit logs (not self-reporting survey measures) to monitor the web activity of employees. In stage 1, a mild AUP reminder sent to company employees resulted in a 12% decrease in employee Internet abuse. In stage 2, a more severe AUP reminder resulted in a 33% decrease in employee Internet abuse. For both stages, the AUP warning (regardless of severity level) resulted in an immediate and significant decrease in employee nonwork Internet use. Results indicate that the severe AUP treatment was more effective in reducing and maintaining lower levels of employee nonwork Internet use than the mild AUP treatment. Under the mild AUP treatment, employee nonwork Internet use levels returned to their pretreatment levels after only one week. However, under the severe AUP treatment, employee nonwork Internet use levels were lower than the mild AUP treatment and remained consistently lower than their pretreatment levels even after three weeks. These results suggest that nontechnical deterrence methods in the form of organizational IT use policies may constitute an effective approach to reducing employee Internet abuse, particularly if AUP policies are clear with regard to related sanctions and penalties for employee noncompliance.

1. Introduction

While computers and the rapid availability of data and information from the Internet have enriched and expanded the personal and professional lives of information workers, (Howard, Rainie, & Jones, 2001; Shu, Tu, & Wang, 2011; Van-Schaik & Ling, 2005), employee technology abuse continues to be a major concern for organizations. Technology abuse can take many forms such as violations of cyber-security policy, breaches of restricted IT resources, piracy of copyrighted information, unauthorized transfer of intellectual property, and employee Internet abuse. Employee Internet abuse, often termed "cyber loafing" or "cyber-slacking," entails employees using organizational resources to access the Internet during work hours for personal purposes (Glassman, Prosch, & Shao, 2015; Henle, Kohut, & Booth, 2009; Vitak, Crouse, & LaRose, 2011). Internet abuse during employee work hours involves various nonwork-related Internet activities such as online chatting, personal customer shopping, personal (i.e., nonbusiness) emails, downloading music, online gaming, blogging, instant messaging, stock trading, online gambling, and various forms of pornography and cybercrime (Henle et al., 2009; Lee & Tsai, 2010; Shepherd, Mejias, & Klein, 2014; Vitak et al., 2011). It is estimated from 63% to 80% of employees use the Internet during work hours for personal purposes, with some employees spending 10 hr or more per week engaged in nonbusiness-related Internet activities (Conner, 2013). Such abuse generates a discernible loss of productivity for both employees and organizations (Henle et al., 2009; Shih, Hsu, Yen, & Lin, 2012; Siponen & Vance, 2010). Additionally, Internet abuse and cyber loafing tie up network and transmission bandwidth, degrade system performance, and increase the legal liability for organizations in terms of copyright infringement, intellectual property theft, and the downloading of unlicensed software (D'Arcy & Devaraj, 2012; Henle et al., 2009; Young & Case, 2004).

Internet abuse has shown a high correlation with the introduction of malware viruses, spyware, key loggers, Trojan horses, password cracking exploits, rootkits, and a host of other cyber threats that compromise IT systems and facilitate the unauthorized breach of intellectual property and data (Kolkowska & Dhillon, 2013). In many cases employees do not perceive the personal use of the Internet as wrong and are quick to justify their Internet behavior (Kim & Yong, 2012; Lee & Tsai, 2010; Pfleeger & Caputo, 2012; Van Schaik & Ling, 2005). Maintaining the confidentiality, integrity, and security of information resources is considered a top priority by organizations and a significant amount of research has investigated the relationship between IT security and employee work behavior (Bulgurcu, Cavusoglu, & Benbasat,

CONTACT Morgan M. Shepherd ✉ mshepher@uccs.edu College of Business, University of Colorado–Colorado Springs, 1420 Austin Bluffs Parkway, Colorado Springs, CO 80918, USA.

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/hihc.

2010; D'Arcy & Devaraj, 2012; Shih et al., 2012; Siponen & Vance, 2010). Subsequently, there has been increased attention focused on compliance with federal and organizational IT use policies and the abuse of IT resources by employees (Shih et al., 2012; Warkentin, Johnston, & Shropshire, 2011). While it is not clear as to where the pendulum swings along the "beneficial use versus abuse" continuum regarding Internet access, it is reasonable to assume that employee Internet abuse is detrimental to organizations on several levels (Shepherd & Klein, 2012; Shih et al., 2012).

Organizations have attempted to reduce employee Internet abuse by the use of monitoring and the enforcement of IT acceptable use policies (AUPs) via sanctions and penalties for employee noncompliance (Pfleeger & Caputo, 2012; Shih et al., 2012). Given the high probability of a security breach due to employee Internet abuse, it would be prudent to investigate methods to manage and reduce its occurrence and minimize a range of potentially negative outcomes (Glassman et al., 2015; Henle et al., 2009; Kolkowska & Dhillon, 2013; Warkentin et al., 2011).

The current article summarizes the results of a two-stage longitudinal study that investigates employee Internet abuse and how it can be reduced by nontechnical deterrence methods, specifically via organizational AUPs. The first stage of the study utilized a "mild" AUP reminder to employees that organizational IT resources were to be used for business purposes only. In the second stage, conducted approximately one year later, a more "severe" AUP reminder informed employees that their Internet activity was being monitored and that penalties and sanctions would be imposed for employee noncompliance to the AUP policy. The results of these two field experimental treatments were analyzed to determine their respective effects on deterring or reducing the level of employee Internet abuse. Of note is that much of the prior research regarding IT use policies and deterrence measures for employee noncompliance regarding Internet abuse relied upon perceptual or self-reported surveys. The current research utilized actual employee Internet usage data and aggregate audit logs to analyze the effect of nontechnical deterrence measures upon employee nonwork Internet usage. We believe that this study makes a needed contribution to the literature in the areas of deterrence theory and the effects of nontechnical deterrence methods upon employee Internet abuse.

In the following sections of the article we review the literature for our theoretical framework, develop a research model and related hypotheses, discuss the research methodology used to test our hypotheses, and finish with a discussion of our results, implications, and conclusion.

2. Prior Research and Theoretical Framework

Prior research has examined several approaches to addressing and mitigating employee Internet abuse. These methods include establishing "acceptable use policies" (AUP) with regard to appropriate Internet usage (Glassman et al., 2015; Shepherd & Klein, 2012), generating employee awareness via SETA (security, education, training, and awareness) programs (Mejias & Balthazard, 2014; Mejias & Harvey, 2012), and enforcing employee compliance via deterrence measures (D'Arcy & Devaraj, 2012; D'Arcy, Hovav, & Galletta, 2009; Herath & Rao, 2009). The incorporation of formal employee AUP with regard to Internet use is frequently utilized as a form of cyber security to enforce employee compliance (Bulgurcu et al., 2010). Since compliance with IT use policies is essential to strengthening IS security, understanding compliance behavior is crucial for leveraging organizational human capital (Bulgurcu et al., 2010; Pfleeger & Caputo, 2012) and raising employee awareness to the dangers related to Internet abuse (Henle et al., 2009; Mejias & Harvey, 2012).

Underlying the need to enforce employee compliance and reduce Internet technology abuse has been the concept of *deterrence*. Deterrence has been defined as the use of punishment or consequences to deter individuals from committing some prohibited, restricted, or illicit activity (Becarria, 1963; D'Arcy & Devaraj, 2012; D'Arcy & Herath, 2011). Much of the prior research in IT deterrence focuses on fear-based mechanisms, formal sanctions, and punishment for employee noncompliance (D'Arcy & Devaraj, 2012; D'Arcy et al., 2009). While the extant research affirms the effectiveness of sanctions and punishment as effective deterrents, a substantial variance remains in many studies indicating that deterrence theory alone may not provide a complete understanding of technology misuse (D'Arcy & Devaraj, 2012). Within this context we considered previous Information System (IS)-related theoretical frameworks to better understand how employee Internet abuse may be mitigated or deterred.

There are numerous theory-based and empirical-based studies on employee technology use, compliance, and deterrence, suggesting that this area of research is becoming increasingly important (D'Arcy & Devaraj, 2012; Herath & Rao, 2009; Shih et al., 2012; Shu et al., 2011) to both researchers and practitioners. For the current study we found three theoretical frameworks that may complement the deterrence literature in understanding employee Internet abuse. Our research found that *General Deterrence Theory* (GDT) (Beccaria, 1963; D'Arcy & Herath, 2011), *Rational Choice Theory* (RCT) (Becker, 1974; D'Arcy & Devaraj, 2012), and *Agency theory* (Eisenhardt, 1989; Jensen & Meckling, 1976) provided relevant theoretical frameworks for the current study in understanding technology abuse and deterring employee Internet abuse in particular.

All three theoretical frameworks possess components that consider penalties and consequences for noncompliance behavior in the workplace. Since GDT is based in part on many of the precepts of RCT, there were several areas of commonality that proved insightful in understanding employee Internet abuse, compliance, and deterrence. Both GDT and RCT provide similar components that consider the severity of the deterrent (e.g., cost, penalty) against the illicit behavior and the probability that such a cost or penalty will be administered. Agency theory complements this commonality with GDT and RCT by seeking to explain "compliance" in relation to communication uncertainty and goal incongruence. All three theories seek to understand appropriate IT use behavior (i.e., compliance with IT use policies) and seek to provide incentives or deterrents to encourage appropriate employee workplace behavior.

2.1. General Deterrence Theory

Deterrence theory is one of the most widely applied theories related to behavioral IS studies and provides a prominent theoretical perspective to employee Internet abuse (D'Arcy & Devaraj, 2012; D'Arcy & Herath, 2011). *Classical* deterrence theory focuses on formal or legal sanctions that seek to prevent or discourage potential offenders from behaving in a particular manner (Gibbs, 1975). GDT posits that the greater the perceived certainty, severity, and swiftness of sanctions imposed upon an individual for an illegal or illicit act, the more individuals will be deterred from committing that act (Beccaria, 1963; D'Arcy & Herath, 2011). *Contemporary* deterrence theory is based upon a "rational choice" view of human behavior and posits that individuals will first consider the anticipated risks, penalties, and costs of any formal or informal sanctions before deciding on whether or not to engage in a particular unauthorized or illicit activity (D'Arcy & Herath, 2011; Pratt, Cullen, Blevis, Daigle, & Madensen, 2006). Research has used deterrence theory as a theoretical foundation to predict employee behavior in the workplace that may be supportive or noncompliant with organizational AUP and IS security policy (Chen, Ramamurthy, & Wen, 2012; D'Arcy & Herath, 2011).

The mechanisms for deterrence consist of two dimensions: detection probability (or certainty) and sanction severity (Paternoster & Simpson, 1996; Wenzel, 2004; Li, Zhang & Sarathy, 2010). Both dimensions are related to an individual's *perception* of the probability that they will be "caught" committing an unauthorized or illicit activity rather than their perception of the *actual detection* probability and related severity of sanctions. Therefore, there are two key assumptions that underline the concept of deterrence: (1) that specific punishments imposed on offenders will deter or prevent individuals from committing further crimes; and (2) that the fear of such punishment will prevent others from committing similar crimes or illicit activities (D'Arcy & Devaraj, 2012; D'Arcy & Herath, 2011).

Deterrence may refer to both technical and nontechnical measures. *Technical* measures refer to access control, strong passwords, firewalls, antivirus software, encryption, intrusion detection systems (IDSs), and redundant networks to name a few (Mejias & Balthazard, 2014; Sawik, 2013; Whitman & Mattord, 2012). *Nontechnical* measures refer to employee Internet use policies, SETA programs that educate employees of the cyber-attack implications of noncompliance (Ciampa, 2012; Mejias & Balthazard, 2014; NIST, 2006), and the monitoring of employee activity via audit logs. However, when user audit logs and IT video monitoring are employed to track employee compliance with organizational IT use policies, research studies have shown that workplace satisfaction decreases when these particular types of deterrence measures are employed (Shepherd et al., 2014). Nontechnical remedies may also refer to legal actions such as prosecution, incarceration, fines, and employment termination. Despite its solid foundation in criminology and empirical research, deterrence theory may not fully explain the phenomenon of employee Internet abuse (D'Arcy & Herath, 2011; Paternoster & Simpson, 1996; Pratt et al., 2006).

2.2. Rational Choice Theory

The Pasternoster–Simpson model of corporate crime, also known as the RCT, is based upon the subjective and theoretically expected utility or benefit of an outcome (Paternoster & Simpson, 1996). RCT uses a neoclassical economic approach to explain how individuals make decisions when faced with various options (Bulgurcu et al., 2010). RCT suggests that potential offenders consciously consider the related costs and benefits in deciding whether to commit a particular deviant or illicit act (Beccaria, 1963; Bulgurcu et al., 2010; D'Arcy & Herath, 2011). RCT has two basic assumptions: (1) that decisions to commit an illicit act consider both the costs (i.e., penalties) and the benefits of the act; and (2) that this decision is affected by the decision-maker's *perceived* expectations of the related benefits and cost of that act (Li et al., 2010). For example, Becker (1974) states that a criminal will adopt a rational and economic choice perspective by seeking to maximize their expected benefit(s) from an illicit or illegal activity that, hopefully, will be in excess of the expected cost of punishment. In essence, the intention to commit corporate crime or illicit activity within an organizational setting may be the function of the following factors (Paternoster & Simpson, 1996):

- Perceived benefits of the action for oneself
- Perceived formal sanctions directed against oneself
- Perceived informal sanctions directed against oneself
- Feelings of shame or self-imposed punishment
- Moral inhibitions against committing the act
- Perceived benefits of the action for the firm
- Perceived formal sanctions directed against the firm
- Perceived informal sanctions directed against the firm
- Perceived loss of prestige for the firm
- The organizational context of the firm

RCT provides a foundation for GDT and would be useful in understanding employee Internet abuse, compliance, and deterrence, particularly with regard to the white collar workers in our study. With regard to Internet technology abuse, employees may likely abuse Internet access if the related risks and costs can be justified by the perceived benefits from engaging in Internet abuse. Because RCT provides a concise and logical explanation of rational decision-making, it has been adapted to various individual, social, and economic contexts to explain a range of deviant behaviors such as income tax evasion, juvenile delinquency, theft, drunk driving, and the motivation behind corporate crime or white collar crime (Bulgurcu et al., 2010; Li, Zhang, & Sarathy, 2010; McCarthy, 2002; Paternoster & Simpson, 1996).

However, some major shortcomings of RCT include the fact that employees are strongly influenced by their individual preference and perception of relative costs and benefits (Bulgurcu et al., 2010; Becker, 1974). Additionally, the relative "costs" and "benefits" perceived by the individual decision-maker may not always be monetary in nature; they could be cultural, social, or behavioral (Bulgurcu et al., 2010; McCarthy, 2002). Since users are the weakest link in information systems, deviant behavior by individuals continue to constitute the biggest impact on the security of an organization when employees visit nonwork-related websites and download nonwork-related software (Li et al., 2010). In this context, an employee's decision whether to comply with an organizational AUP or engage in unauthorized and deviant behavior (i.e., employee Internet abuse) may constitute a real threat to organizational productivity and cyber security.

2.3. Agency Theory

The most common form of Agency theory (aka the Principal–Agent theory) is when the owner (principal) of organizational resources hires or employs another party (agent) to perform some prescribed work or task according to a mutually agreed contract (Eisenhardt, 1989). Agency relationships are instituted whenever one party depends on another party to undertake or complete some action on their behalf (Jensen & Meckling, 1976). If such an agreement is made under uncertainty (due to incomplete information or poor communication), between the principal and the agent, information asymmetry and goal incongruence about intended goals occur (Eisenhardt, 1989; Glassman et al., 2015). Specifically, the goal(s) of the agent may prove to be inconsistent with the goal(s) of the principal. Information asymmetry puts principals (i.e., organizations) at a disadvantage because they are faced with a pool of agents (i.e., employees) who are exhibiting undesirable characteristics (i.e., employee Internet abuse).

Goal incongruence in Agency theory with regard to employee Internet abuse also occurs when an employee (agent) uses the principal's resources (i.e., company Internet resources) for cyber loafing, which is in conflict with the goals and productivity of the employer (agent). Several methods to address this agency problem with regard to employee Internet abuse include monitoring employee web activities, maintaining audit logs that record the websites that employees have visited, and developing white lists (work appropriate) and black lists (nonwork inappropriate) for organizational websites (Eisenhardt, 1989; Glassman et al., 2015; Herath & Rao, 2009; Shih et al., 2012). Agency theory contributes to our understanding of the need to address cyber loafing to verify appropriate behavior in the workplace and deter IT and employee Internet abuse. Agency theory has also been used to explain compliance with information security policies with regard to noncompliance penalties, social pressure from fellow workers, and the perceived effectiveness of one's security behaviors (Herath & Rao, 2009; Li, Zhang & Serathy, 2010).

Agency theory, however, is limited in its explanatory power. Specifically, principals (i.e., owners) delegate authority or responsibility to a manager who acts on their behalf. However, managers who act on behalf of principals often cannot easily monitor their agents (i.e., employees) and enforce expected actions (i.e., compliance with AUPs). Cyber loafing and other forms of employee Internet abuse may occur because organizations do not specifically address this particular agency problem and, subsequently, do not verify whether employees have been using Internet resources appropriately Glassman et al., 2015).

3. Research Model and Hypotheses

While any viable information security program incorporates the implementation of both technical and nontechnical controls, *nontechnical* deterrence measures have been shown to be cost-effective in preventing employee IT abuse (D'Arcy & Herath, 2011; Mejias & Balthazard, 2014; Png, Wang, & Wang, 2008). In addition to SETA programs, ISA (information security awareness) initiatives and Internet AUPs that monitor employee activity have been shown to be effective in reducing various types of employee Internet abuse (Bulgurcu et al., 2010; Henle et al., 2009). Internet use policies and related sanctions are considered to be the first line of deterrence or intervention in encouraging employees to become mindful of the appropriate use of organizational IT resources (Li et al., 2010; (Johnson & Ugray, 2007; Kolkowska & Dhillon, 2013). In the following section we examine the use of two nontechnical deterrence measures and their respective effects upon reducing nonwork Internet traffic *as a form of employee Internet abuse*. We discuss the effect of *reminders* of an AUP and the *severity* of the AUP message with regard to how it may affect the *frequency* and the *longevity* effect of employee Internet abuse as depicted in Figure 1, our General Research Model.

3.1. User Reminders of AUP Policy

The monitoring and surveillance of employee Internet usage have been found to be effective in decreasing employee Internet abuse (Henle et al., 2009; Herath & Rao, 2009). However, researchers have suggested that organizations also consider technology use policies as a deterrent to minimize employee Internet abuse (D'Arcy et al., 2009; Herath & Rao, 2009; Kolkowska & Dhillon, 2013). However, such policies must be immediately communicated to correct behaviors that affect employee Internet abuse judgments. Numerous studies indicate that reminding organizational users of technology use policies and related sanctions for noncompliance generates a significant impact upon user behavior and ethical conduct (D'Arcy & Herath, 2011; Kolkowska & Dhillon, 2013; Warkentin et al., 2011).

RCT affirms that formal sanctions and penalties constitute an important instrument for deterring deviant behavior (Kolkowska & Dhillon, 2013). Other researchers state that organizational IT polices are not likely to improve ethical behavior. Simply obliging employees to sign an AUP agreement may not reduce employee Internet abuse (Glassman et al., 2015; Li et al., 2010). More commonly, employees may not be fully informed or read the content and details of their organization's Internet use policies (D'Arcy & Devaraj, 2012). GDT suggests that policies, like laws, are effective only when

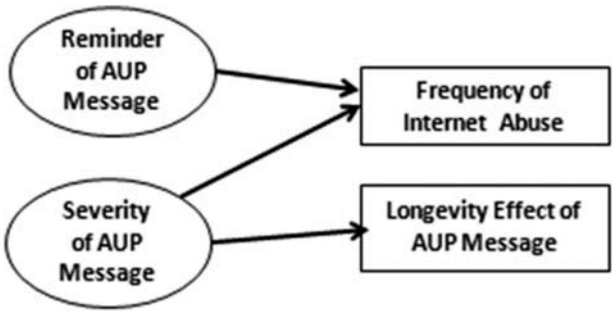

Figure 1. General research model.

informational content is clearly *communicated* to its organizational users (D'Arcy & Herath; Ciampa, 2012).

Agency theory suggests that the lack of perfect or complete information between the principal (i.e., organization) and the agent (i.e., employee) often results in information asymmetry regarding the appropriate use of organizational resources (i.e., Internet), which may result in employee Internet abuse or cyber loafing (Glassman et al., 2015; Shepherd et al., 2014). However, RCT assumes that potential violators of IT use policies are well informed of efforts (e.g., AUP reminders) to control noncompliant behaviors (Peace, Galletta, & Thong, 2003). If employees have been informed that related penalties for noncompliance are being enforced, employees would more likely comply with such IT use policies (D'Arcy & Devaraj, 2012; Herath & Rao, 2009). Therefore, it would be reasonable to assume that employees receiving an AUP reminder would be more likely to comply with such an organizational IT use policy, particularly with regard to Internet use. Therefore, we propose the following hypothesis.

H1: A reminder to employee Internet users, that organizational AUPs are in effect, will immediately reduce the frequency of employee Internet abuse.

3.2. Severity of AUP Message

RCT and GDT posit that the greater the perceived severity of sanctions (i.e., cost of the penalty) for an illicit act, the more likely individuals are deterred from committing that act (D'Arcy & Devaraj, 2012). Additional research indicates that employee nonconformance to organizational IT use policies can be deterred by imposing *severe* penalties (D'Arcy & Devaraj, 2012; Herath & Rao, 2009). With regard to employee Internet abuse, studies suggest that aggressive ISA programs that remind employees of severe penalties and sanctions for noncompliance will affect employee Internet abuse (Henle et al., 2009; Herath & Rao, 2009). According to RCT, the *perceived severity* of a sanction exerts an important influence in deterring unwanted or deviant behavior (D'Arcy & Devaraj, 2012). High levels of perceived severity increase the *perceived cost* of deviant behaviors and may counteract the perceived benefit of a deviant behavior (D'Arcy & Herath, 2011).

Based upon these research findings, we anticipate that employee IT abuse, in the form of nonwork Internet use, will reduce in frequency as the severity of the AUP message increases. Therefore, we propose that a more severe AUP message with related and stated sanctions would increase the perceived cost (i.e., penalty) of employee noncompliance and reduce the frequency of employee Internet abuse.

H2: The frequency of employee Internet abuse will decrease, as the severity of the AUP notice increases.

3.3. Longevity Effect of AUP Message

A review of the related literature regarding the role of sanctions and the severity of penalties in deterring deviant acts suggest that as the severity level of sanctions increases, individuals may be less inclined to carry out a particular deviant act (D'Arcy & Devaraj, 2012; Herath & Rao, 2009). The severity of the organizational IT use policy may also have a mitigating effect on the duration or *longevity* of the employee Internet abuse (Chen et al., 2012; Li et al., 2010; Johnson & Ugray, 2007). Organizational IT use policies traditionally contain specific policies and employee responsibilities with regard to safe computing and the appropriate use of organizational IT resources. ISA and SETA programs actively seek to increase employee awareness of the dangers to the entire organization of unsafe computing and the related penalties (including employment termination) that will be imposed upon employees for noncompliance (Mejias & Balthazard, 2014; Mejias & Harvey, 2012). It would be reasonable, therefore, to assume that a more severe AUP message to employees regarding the consequences and penalties for noncompliance would generate a longer longevity effect, of reducing the duration of employee Internet abuse, than a mild AUP message. Therefore, we hypothesize that:

H3: A severe AUP message reminder will generate a longer-duration effect in reducing the frequency of employee Internet abuse than a mild AUP message.

4. Research Methodology

Much of the previous research regarding employee IT Internet abuse has focused on short-term studies to determine whether users responded to a particular single or one-time experimental treatment (Glassman et al., 2015). The research methodology in the current study was composed of two longitudinal studies (i.e., stage 1 and stage 2) that were conducted approximately one year apart. Stage 1 of the study utilized 200 white collar employees from the areas of accounting, finance, and human resources. Stage 2 used a nearly identical employee pool of the same 200 employees with only minor personnel changes (<1% in turnover). For both stages of our study the identity of our organization and its related industry were kept confidential as a condition for the data collection for our research. The procurement and compiling of the field experimental data were problematic and time consuming as researchers were required to constantly provide assurances to the CIO and upper management that employee web traffic and Internet activity would not be tracked to individual users. Therefore, we were not allowed to divulge much about the company in the reporting of our research results. We were allowed to write that all employees in both stages were working professionals from a small-to-medium (SME)-sized service-oriented enterprise located in the mid-western United States. So that the employees would not be aware that this research was ongoing, we did not survey them for demographic data. We can report that, from visual observation, about 75% of the employees were young to mid-career, white collar, accounting, finance, and HR professionals.

All employees were required to complete a company-provided SETA training, which was offered as an online program before the research was conducted and employees had to review the AUP. Although no data could be tracked back to any individual employee, Institutional Review Board (IRB) approval was nevertheless obtained for this research.

Two experimental treatments were used: a mild AUP message (stage 1) and a severe AUP message (stage 2). The experimental treatments were administered in the form of a one-time, pop-up company AUP notice that appeared when employees logged on. The one-time, pop-up AUP notice was sent to all 200 employees in our study as well as to the organization's IT department. For the stage 1 study (i.e., mild AUP experimental treatment), the one-time pop-up AUP message gently reminded employees that the company's IT resources were to be used for business purposes only, as stated below:

> Please remember that <company> systems are to be used for business purposes only.

The stage 2 portion of our study was conducted approximately one year later. For the stage 2 study (i.e., severe AUP experimental treatment), the one-time, pop-up AUP notice conveyed a more severe AUP message. It informed employees that their Internet activity was being monitored and that sanctions and penalties would be imposed for employees that did not comply with the company's AUP policy:

> The IT department has recently been tracking an increased amount of web activity over our networks. Please remember that <company> IT policy prohibits personal use of <company> computing resources and that <company> reserves the right to restrict or revoke computing privileges of those who abuse the policy.

4.1. Data Collection

Our experiment used *Splunk©* software, a log monitoring and data reporting search tool, for analyzing the websites visited by the IP addresses of the employees in our sample research pool. Individual IP addresses remained static throughout the research study and the data was not tracked back to individual employees. Employee Internet usage was monitored during the first week of the study (on a Thursday) before any experimental treatments were administered to establish a *baseline* level of employee Internet traffic activity. This baseline constituted the *preexperimental* data point. Five days later, on the following Tuesday, AUP reminders were sent to all employees. The experimental treatments for both stage 1 (mild AUP treatment) and stage 2 (severe AUP treatment, 1 year later) were administered only *once*, on that Tuesday before any experimental treatments were administered, and were not repeated for any subsequent weeks. We allowed two days for the message to be viewed by all employees in our subject pool. The first data reading (D1) was collected and analyzed on the Thursday, two days after the initial AUP reminder. At this point in the study, we had established our previous baseline Thursday reading, our Tuesday treatment, and the first post-treatment reading (D1).

Subsequent data collections were taken on Thursdays of the following work week to ensure similar business practices, to minimize any "day-of-the-week" confounds, and to maintain data collection consistency related to a particular weekday. That is, observations and data collection (D2, D3) for each stage of the experiment were continued for the successive two Thursdays of the following weeks. Additionally, our two-stage study was conducted in early spring to avoid confound effects from any seasonal cycles or the closing of any fiscal periods or any other extraordinary business cycles. The company's IT group activated the Splunk© software and collected all Internet usage data from the employee pool. The Splunk© software ran for 24 hr each day.

As an additional control to reduce the potentially confounding effect of whether employees were visiting nonwork Internet websites during their lunch hour (i.e., approximately 12:00 pm to 1:00 pm), only employee Internet usage data collected between 9:00 am and 11:00 am was included in our analysis. This experimental control was employed to restrict the data analysis of employee Internet behavior to normal working hours. Of note is that there were no major national or world events occurring in the news media or within the company during the experimental time frame for which employee data was collected for both stage 1 and stage 2 of the study. All data were collected at the aggregate level to assure employee privacy and confidentiality.

We grouped the various websites that employees visited into five categories (see Table 1). Category 1 (Business-related) represented websites generally considered to be used for work and business-related purposes. The majority of this employee Business-related traffic originated from the company's network servers. While researchers could not see actual screen shots of the websites visited by employees, we were able to ascertain by the URLs and related audit usage logs whether employees were visiting a company or business-related location (e.g., the accounting department's web page on the corporate server). Category 2 (Mixed) represented various websites that *could* be considered to be work-related. A large percentage of websites in this category were social networking and informational websites such as Facebook, LinkedIn, Google, or Wikipedia.

While social networks are frequently utilized by company HR departments to review potential job candidates, inclusion of these websites may have potentially skewed employee Internet data results away from the "Nonwork" category. Category 3 (Neutral) was used to represent routine employee Internet traffic generated by web surfing such as company server hits, marketing ads, and search engine traffic. As this type of Internet traffic and usage may be generic to all web surfing and Internet search inquiries, these particular websites were categorized as Neutral. Category 4 (Tunes) referred to online music websites and constituted a very small percentage of overall employee Internet use (< 3%). Category 5 (Nonwork), which was the focus of our research study, consisted of all employee Internet usage that

Table 1. Category descriptions.

Category	Description
1. Business-related	Site related to business activities
2. Mixed	Social networking sites (some of these might be business related)
3. Neutral	Routine employee network traffic, web and company server hits, search engine traffic
4. Tunes	Online music sites
5. Nonwork	Nonbusiness-related sites

was not directly or indirectly work or business related. Examples of employee nonwork Internet traffic would be professional sports sites, online shopping, Internet gambling, personal stock trading, online department stores, style and fashion sites, and Hollywood gossip sites to name a few.

5. Results

The total number of websites visited during each data collection was approximately 55,000 for stage 1 (mild AUP treatment) and 45,000 for stage 2 (severe AUP treatment). For both stages our initial results revealed that the *network* component of Category 3 ("Neutral") constituted the majority of the websites visited by employees. As our research study was designed to focus only on employee work-related (i.e., Category 1 "Business-related") and nonwork Internet websites (Category 5 "Nonwork"), we removed Category 2 ("Mixed"), Category 3 ("Neutral"), and Category 4 ("Tunes") data from our data analysis for parsimoniousness. The remaining tallies for the "Business-related" and "Nonwork" categories websites for both stage 1 and stage 2 were consistently around 17,000 sites for each stage of the study.

Table 2 displays the results generated from the stage 1 (mild AUP reminder) experimental treatment. Data was collected over four time periods: one pretreatment and three posttreatment readings (D1, D2, and D3). As discussed in the Methodology section, the Pretreatment reading refers to the baseline week where no AUP experimental treatment was given. The D1 data reading refers to the data collected on the Thursday after the baseline (pretreatment) week and two days after the first one-time AUP message treatment, which was administered on the Tuesday during the second week of the study for both stages. Data readings D2 and D3 were also collected on the following Thursdays. Results for the stage 1 study (mild AUP notice) show that the percentage of nonwork Internet use as a form of employee Internet abuse was relatively high (55%) at the pretreatment period before the introduction of the mild AUP experimental treatment message. At the posttreatment reading, D1, employee nonwork Internet usage immediately decreased from 55% to 43%. However, for the posttreatment readings at D2 and D3, employee nonwork Internet use returned to its approximate pretreatment levels.

Table 3 displays the results generated from the stage 2 (severe AUP notice) experimental treatment, conducted one year after the stage 1 study. Data was collected over four time periods: one pretreatment and three posttreatment readings (D1, D2, and D3). All previous experimental conditions used for the stage 1 study were replicated for stage 2 (i.e., data was collected on Thursdays). Table 3 illustrates the significant and immediate effect of the severe AUP message upon the pretreatment employee nonwork Internet usage level as a form of employee Internet abuse. At the D1 reading employee nonwork Internet usage decreased from 72% to 39%. For reading D2, the percentage of employee nonwork Internet usage increased to 50%, but still remained below the pretreatment level. By the D3 reading, the percentage (59%) of employee nonwork Internet usage increased slightly from D2 but continued to remain lower than the pretreatment level. Specifically, three weeks after the one-time severe AUP notice treatment was administered, employee nonwork Internet usage still remained below the pretreatment level of 72%. The contrast of the effects of the two experimental treatments (mild AUP versus severe AUP notices) is depicted in Figure 2.

Table 2. Stage 1 (Mild AUP Notice) % Internet usage.

Category	Pretreatment	D1 Reading	D2 Reading	D3 Reading
Business	45%	57%	40%	43%
Nonwork	55%	43%	60%	57%

Table 3. Stage 2 (Severe AUP Notice) % Internet usage.

Category	Pretreatment	D1 Reading	D2 Reading	D3 Reading
Business	28%	61%	50%	41%
Nonwork	72%	39%	50%	59%

Results from the stage 1 (mild AUP) treatment indicate that the level of employee nonwork Internet use decreased from its pretreatment level of 55% to 43% in the two days after the mild AUP treatment was administered (see Table 2). Results from the stage 2 (severe AUP) treatment (see Table 3) indicate a greater and more significant decrease in employee nonwork Internet use from its pretreatment level of 72% to 39% in the two days after the severe AUP treatment was administered. For both stage 1 and stage 2, a test of proportions also indicated that the percentage of Business-related website visits increased while the proportion of employee nonwork visits decreased after the introduction of either AUP message treatment ($p < .05$).

All statistical tests of the hypotheses were conducted with a Chi-square test of proportion differences using Medcalc. For Hypothesis 1, both stage 1 and stage 2 results were examined to determine whether the AUP reminder to employees reduced the frequency of employee nonwork Internet usage from their pretreatment levels. For both stages, the level of employee nonwork Internet use was significantly less in D1 ($\chi2 = 489$, $p < 0.0001$) for the stage 1 study and significantly less in D1 ($\chi2 = 1120$, $p < 0.0001$) for the stage 2 study compared with their pretreatment levels. For hypothesis 2, the decrease in frequency for employee nonwork Internet use from the stage 2 treatment (severe AUP notice) was statistically greater than the stage 1 treatment (mild AUP

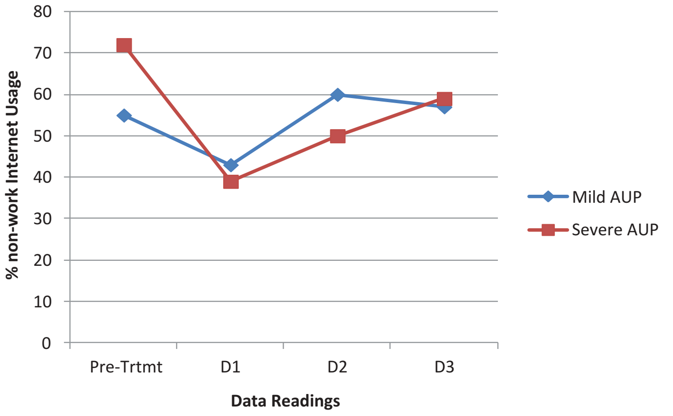

Figure 2. Nonwork Internet usage percentages.

notice) (χ2 = 788, $p < 0.0001$). For hypothesis 3, the reduction in employee nonwork Internet use was statistically greater for the severe AUP treatment than for the mild AUP treatment for D1 (χ2 = 12493, $p < 0.0001$) and D2 (χ2 = 8498, $p < 0.0001$). Therefore, all hypotheses proposed in our study were supported.

6. Discussion

6.1. Hypothesis 1

The results of our hypotheses testing are summarized in Table 4. Our field experimental results support Hypothesis 1: *A reminder to employee Internet users that organizational AUPs are in effect will immediately reduce the frequency of employee Internet abuse*. For both stages 1 and 2 of the study, the percentage of employee nonwork Internet usage immediately decreased following the introduction of either the mild AUP or severe AUP treatments. For stage 1 (mild AUP notice) the percentage of employee nonwork Internet usage immediately decreased by 12% ($p < 0.05$) from its pretreatment level of 55% to 43% (D1) following the introduction of the mild AUP reminder. However, the reduction in employee nonwork Internet usage was not sustained for subsequent mild AUP treatment readings D2 and D3 (administered two and three weeks after the mild AUP treatment). For the mild AUP treatment, employee nonwork Internet use returned to its approximate pretreatment levels for D2 (60%) and D3 (57%).

For stage 2 (severe AUP message) conducted one year later, employee nonwork Internet use immediately decreased by 33% ($p < .05$) from its pretreatment level of 72% to 39% (D1). However, as was indicated in stage 1, a sustained reduction in employee nonwork Internet usage was not maintained for the D2 and D3 posttreatment readings. Specifically, reading D2 (50%) was higher than its previous D1 level (39%). D3 (59%) was also higher than the previous D2 level (50%), but still below the pretreatment level of 72%. However, unlike the results for the mild AUP treatment, employee nonwork Internet use for the severe AUP treatment remained below their pretreatment level.

For Hypothesis 1, these results may be partially explained by several factors. The initial AUP reminder to employees may have generated a renewed awareness that employee Internet behavior was now being monitored. Subsequently, both mild and severe AUP treatments generated an immediate and significant decrease in employee nonwork Internet use, following the introduction of either the mild or severe AUP message. However, after the AUP messages were introduced, the "novelty" effect of the AUP may have attenuated. Since AUP "reminders" were introduced only once for both stages of the study and additional AUP message reminders were not sent, employees might have reverted to their previous nonwork Internet use behavior. Subsequently, as seen in Figure 2, employee nonwork Internet use for under both the mild and severe AUP treatments gradually increased in the following weeks after the initial AUP message treatment was introduced.

Agency Theory may be used to explain that the absence of *continued* employee AUP reminders may have contributed to a lack of perfect information about the intended goals of the principal (the organization) and the agent (employee Internet user), thus generating goal incongruence. Specifically, agency problems of this type (i.e., Internet abuse) emphasize the necessity of communicating organization information to employees regarding the appropriate use of IT resources particularly, with regard to employee nonwork Internet abuse (Glassman et al., 2015). GDT could also be used to explain the immediate decrease in employee nonwork Internet use for both experimental treatments. GDT maintains that if organizational IT use policies (i.e., AUPs) are *communicated* to employees, potential violators may be deterred (albeit, temporarily for the mild AUP treatment) from visiting nonwork Internet websites and violating organizational IT use policy (D'Arcy & Herath, 2011; Kolkowska & Dhillon, 2013; Warkentin et al., 2011).

Table 4. Summary of results.

	Hypothesis	Supported
H1	A reminder to employee Internet users, that organizational acceptable use policies (AUP) are in effect, will immediately reduce the frequency of employee Internet abuse.	Yes
H2	The frequency of employee Internet abuse will decrease, as the severity of the AUP notice increases.	Yes
H3	A severe AUP message reminder will generate a longer-duration effect in reducing the frequency of employee Internet abuse than a mild AUP message.	Yes

6.2. Hypothesis 2

Our results support Hypothesis 2 *(The frequency of employee Internet abuse will decrease, as the severity of the AUP notice increases)*. Figure 2 contrasts the profound effects between the two experimental treatments (mild AUP versus severe AUP). As illustrated in Figure 2 and Table 3, while the stage 2 study (severe AUP notice) started with a higher pretreatment level of employee nonwork Internet usage (72%) than the stage 1 study (mild AUP notice) at 55%, the more severe AUP generated a significantly greater decrease ($p < 0.05$) in employee nonwork Internet use than did the mild AUP message. Additionally, employee nonwork Internet usage for the severe AUP message treatment did not return to its pretreatment levels as did the mild AUP message treatment.

These differences in employee nonwork Internet use may be partially explained by GDT particularly, with regard to the greater perceived certainly and severity of the sanctions for noncompliance contained in the severe AUP message. While the mild AUP message ("Please remember that <company> systems are to be used for business purposes only.") correctly restated the organizational IT use policy, it did not state any consequences for noncompliance. In fact, the mild AUP message did not state anything at all about sanctions or penalties for noncompliance. RCT suggests that employees may have perceived that a greater benefit (with no perceived penalty cost) could be derived by continuing to violate the organization's AUP by visiting nonwork Internet websites. Since the mild AUP message treatment in stage 1 of the study did not convey any perception that AUP noncompliance would be detected *or* that sanctions and penalties would be imposed, employees quickly reverted to their pretreatment levels of nonwork Internet use after two weeks.

In contrast, the severe AUP message in the stage 2 study clearly communicated the perception that employee Internet activity was not only being monitored, but that sanctions and penalties would most likely be imposed for employee noncompliance. The severe AUP message generated the perception that violators faced a higher probability of getting "caught" with a greater probability that related consequences and penalties would be imposed. GDT may be used to partially explain the larger percentage reduction in employee nonwork Internet use generated by the more severe AUP message. The severe AUP treatment may have been more effective in creating the perception that imposed sanctions would be a certainty. RCT also suggests that the more severe AUP message appealed to the rational choice decision process of an individual contemplating an illicit act (e.g., employee Internet abuse). Specifically, the monitoring, sanctions, and penalties associated within the severe AUP notice may have been more effective than the mild AUP notice in convincing potential violators that the expected cost of punishment from noncompliance would be in excess of the expected benefit(s).

6.3. Hypothesis 3

Our results support Hypothesis 3. *(A severe AUP message reminder will generate a longer duration effect in reducing the frequency of employee Internet abuse than a mild AUP message.)* While the introduction of either the mild or severe AUP treatment generated an immediate decrease in employee nonwork Internet usage, this effect did not continue and was not sustained for the mild AUP treatment in stage 1 of the study (see Figure 2). In contrast, the severe AUP treatment in stage 2 (which clearly stated that employee Internet activity was being monitored and related sanctions for noncompliance would be imposed) continued to engender a lower level of employee nonwork Internet usage than the mild AUP treatment. Additionally, and unlike the mild AUP message treatment, the percentage of employee nonwork Internet usage under the severe AUP message treatment continued to remain below its preexperimental level for subsequent data readings (i.e., D1, D2, D3).

RCT and GDT may be used to partially explain these results. Not only did the severe AUP message treatment immediately generate significantly lower levels of employee nonwork Internet usage than the mild AUP message treatment, but the sustaining effect of the severe AUP message *continued* to dissuade potential employee Internet abusers long after the initial severe AUP message was administered. With regard to GDT, the severe AUP message may have generated the perception that employee Internet behavior would continue to be scrutinized (i.e., monitored) with a high probability of detection and a high probability that imposed sanctions would be a certainty.

6.4. Limitations

The first limitation refers to the minor attrition rate (< 1%) in our employee data pool that occurred between stage 1 and stage 2 (conducted one year later), which may have generated a small effect upon our results. While the management of the organization in our study assured us that virtually the same employee pool was used for both the stage 1 and stage 2 portions of our study, we believe that this effect, if any, is minimal given the small rate of attrition and the fact that workplace Internet practices are somewhat common across many employee populations and industry samples (Akman & Alok, 2010). The second limitation refers to the lack of an accepted standard or methodology in the IS literature for categorizing which Internet websites should be "Business-" or "Nonwork-related" sites as our results could be affected by this categorization. To reduce the effect of this limitation, we incorporated a conservative approach in our methodology and did not include data from the "Neutral" category. As discussed in our Methodology section, the "Neutral" category represented routine employee network traffic that would be generic to all organizations such as company server hits, marketing ads, and search engine traffic.

Our third limitation refers to the characterization of the "severe" AUP experimental treatment. The severe AUP message, which stated that network web activity was being monitored together with a warning that sanctions and penalties would be imposed for employee noncompliance, may have generated a possible confounding effect for our final results. However, removing the sanctions and penalties component from the severe AUP message would not have differentiated it substantially from the mild AUP message to justify undertaking the stage 2 portion of our study. Our fourth limitation refers to the generalizability of our findings. Since our study was exploratory in nature and used white-collar employees from accounting, finance, and HR from an organization in the service industry, our findings may be less generalizable to a larger or different industry segment. The authors intend to incorporate more subjects from different industries in future research endeavors. Despite these limitations we believe that the results generated by the severe AUP experimental treatment for the stage 2 study generate interesting and useful implications for the effectiveness of nontechnical deterrence methods to reduce employee Internet abuse.

6.5. Implications

Our results generate several interesting implications for researchers and practitioners. First, our results suggest that the use of nontechnical deterrence methods such as IT AUPs may be effective in reducing employee Internet abuse, particularly employee nonwork Internet use. As our results indicate, immediate and significant decreases in employee nonwork Internet usage were generated when either the mild AUP or severe AUP treatments were introduced.

Our second implication refers to the significant effect of the *severe* AUP message as a nontechnical deterrent measure. While both mild and severe AUP treatments generated an immediate and dramatic decrease in employee nonwork Internet usage, the mild AUP treatment did not support sustained and continued lower levels of employee nonwork Internet usage. Conversely, the severe AUP treatment, which clearly communicated that employee Internet activity was being monitored and that penalties would be imposed for employee noncompliance, generated a more significant and sustained decrease in employee nonwork Internet usage. Specifically, employee nonwork Internet usage did not return to their previous pretreatment level as was the case for the mild AUP treatment. This implication is noteworthy since the pretreatment level for employee nonwork Internet usage was initially higher for the stage 1 severe AUP message treatment (72%) than the stage 2 mild AUP message treatment (55%). For practitioners, this finding supports the GDT that effective deterrence measures must generate a clear perception that violators of organizational IT use policies will be detected, and that sanctions and penalties for noncompliance will be certain, swift, and severe (D'Arcy & Herath, 2011; D'Arcy et al., 2009). For both researchers and practitioners that may want to rule out the "novelty" effects of our experimental treatments (i.e., mild versus severe AUP warning), future experimental designs could employ a wider range of severity AUP warnings to determine how employee nonwork Internet usage levels would be affected.

Our third implication refers to the value of clearly communicating organizational IT use policies and penalties for noncompliance. The mild AUP treatment ("Please remember that <company> systems are to be used for business purposes only.") correctly restated the organizational IT use policy. But unlike the severe AUP treatment, the mild AUP treatment did not clearly communicate that employee monitoring of Internet activity would be tracked and that noncompliance would be met with penalties and sanctions. For researchers, this finding is supported by Agency Theory and implies that the lack of perfect or complete information between the principal (i.e., the organization) and the agent (i.e., the employee) may result in information asymmetry or miscommunication regarding the inappropriate use of organizational IT resources (e.g., employee Internet abuse). For practitioners this finding suggests that if employees are not clearly informed and aware of detection efforts and if related penalties for noncompliance are not clearly communicated, that employees are more likely to disobey such IT use policies as there is no perceived fear of "getting caught" or penalized. Finally, since both the mild and severe AUP message treatments were administered only once, at the beginning of each of the two stages of the study, it would be reasonable to suggest that more *frequent* AUP reminders (e.g., continued daily or weekly AUP reminders) could be even more effective in maintaining lower levels of IT abuse in the form of employee nonwork Internet use. This not only implies that organizational IT use policy must be *frequently* and *clearly* communicated to employees but that employee noncompliance would result in related sanctions and penalties.

7. Conclusion

Our results suggest that nontechnical deterrence methods in the form of organizational IT and AUPs may constitute an effective approach to reducing employee IT abuse, particularly with regard to employee nonwork Internet use. Our research study exposed our sample base of 200 white collar employees to both a mild (stage 1) and a severe (stage 2) version of the organization's IT AUP. Across both treatments, the introduction of a one-time reminder of the AUP message generated an immediate and significant decrease in the percentage of employee nonwork Internet use. However, the more severe AUP message, which clearly stated that employee Internet activity was being monitored and that penalties would be imposed for noncompliance, generated significantly lower levels of employee nonwork Internet use than the mild AUP treatment.

However, for both experimental AUP treatments maintaining *continued* lower employee nonwork Internet use was not sustained over time. Specifically, for stage 1 (mild AUP notice), employee nonwork Internet use levels gradually increased and returned to their previous pretreatment levels after a two-week period. For stage 2 (severe AUP notice), employee nonwork Internet use levels also continued to gradually increase. However, employee nonwork Internet use levels for the severe AUP treatment continued to remain below the mild AUP levels and never returned to their pretreatment levels.

Since both the mild and severe AUP messages were administered as a one-time only experimental treatment at the beginning of each stage of the study, it would be reasonable to imply that lower levels of employee nonwork Internet usage were not sustained because more frequent "AUP reminders" were not communicated to employees. When IT use policies are not regularly communicated into the normal business routine of an organization, our study suggests that employee nonwork Internet use may continue or return to their previous pretreatment levels. Conversely, this implies that nontechnical deterrence measures such as organizational IT policies must be periodically and clearly communicated to employees and done so with a high probability that related sanctions and penalties would be imposed for noncompliance. As employee technology abuse in the form of nonwork Internet use constitutes a significant expense in lost labor-hours and related productivity, the authors encourage more research in this area.

References

Akman, I., & Alok, M. (2010). Gender, age and income differences in Internet usage among employees in organizations. *Computers in Human Behavior*, *26*(3), 482–490.

Beccaria, C. (1963). *Essays on crimes and punishment*. New York, NY: Macmillan.

Becker, G. S. (1974). *Essays in the economics of crime and punishment*. Cambridge, MA: National Bureau of Economic Research.

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

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

Ciampa, M. (2012). *Security+ guide to network security fundamentals* (4th ed.). Boston, MA: Course Technology, Cengage Learning.

Conner, C. (2013). *Who wastes the most time at work? Forbes*. Retrieved from http://www.forbes.com/sites/cherylsnappconner/2013/09/07/who-wastes-the-most-time-at-work/

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, *43*(6), 1091–1124.

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

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

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review*, *14*(1), 57–74.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York, NY: Elsevier.

Glassman, J., Prosch, M., & Shao, B. (2015). To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information & Management*, *52*(2), 170–182.

Henle, C. A., Kohut, G., & Booth, R. (2009). Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyber loafing. *Computers in Human Behavior*, *25*(4), 902–910.

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

Howard, P. E., Rainie, L., & Jones, S. (2001). Days and nights on the internet: The impact of a diffusing technology. *American Behavioral Scientist*, *45*(3), 383–404.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360.

Johnson, J., & Ugray, Z. (2007). Employee internet abuse: Policy versus reality. *Issues in Information Systems*, *8*(2), 214–219.

Kim, B. C., & Yong, W. P. (2012). Security versus convenience? An experimental study of user misperceptions of wireless internet service quality. *Decision Support Systems*, *53*(1), 1–11.

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, *33*, 3–11.

Lee, M. C., & Tsai, T. R. (2010). What drives people to continue to play online games? An extension of technology model and theory of planned behavior. *International Journal of Human–Computer Interaction*, *26*(6), 601–620.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*, 635–645.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology*, *28*(1), 417–442.

Mejias, R. J., & Balthazard, P. (2014). A model of information security awareness for assessing information security risk. *Journal of Information Privacy and Security*, *10*, 1–26.

Mejias, R. J., & Harvey, M. (2012). A case for information security awareness programs (ISA) to protect global information, innovation and knowledge resources. *International Journal of Transitions and Innovation Systems*, *2*(3–4), 302–324.

NIST (National Institute of Standards and Technology) (2006). *NIST-100, Technology Administration, U.S. Dept. of Commerce, Information Security Handbook: A Guide for managers, prepared by Bowen, P., Hash, J., & Wilson, M.* Gaithersburg, MD: NIST.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, *30*(3), 549–584.

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

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber-security risk. *Computers & Security*, *31*(4), 597–611.

Png, I. P. L., Wang, C. Y., & Wang, Q. H. (2008). The deterrent and displacement effects of info security enforcement: International evidence. *Journal of Management Information Systems*, *25*(2), 125–144.

Pratt, T. C., Cullen, F. T., Blevis, K. R., Daigle, L. E., & Madensen, T. D. (2006). The empirical status of deterrence theory: A meta-analysis. In In F. T. Cullen, J. Wright, & K. Blevins (Eds.), *Taking stock: Status of criminological theory* (pp. 37–76). New Brunswick, NJ: Transaction Publishers.

Sawik, T. (2013). Selection of optimal countermeasure portfolio in it security planning. *Decision Support Systems*, *55*, 156–164.

Shepherd, M., & Klein, G. (2012). Using deterrence to mitigate employee internet abuse. In *Proceedings of the 44th Annual Hawaii International Conference on Systems Sciences (HICSS)*. Waikola, HI: IEEE.

Shepherd, M. M., Mejias, R. J., & Klein, G. (2014). A longitudinal study to determine the effects of non-technical deterrence on reducing employee Internet abuse frequency. In *Proceedings of the 47th Hawaii International Conference on Systems Sciences* (pp. 3159–3168). Waikola, HI: IEEE.

Shih, D. F., Hsu, S. F., Yen, D. D., & Lin, C. C. (2012). Exploring the individual's behavior on self-disclosure online. *International Journal of Human–Computer Interaction*, *28*, 627–645.

Shu, Q., Tu, Q., & Wang, K. (2011). The impact of computer self-efficacy and technology dependence on computer-related technostress: A social cognitive theory perspective. *International Journal of Human–Computer Interaction*, *27*(10), 923–939.

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

Van Schaik, P., & Ling, J. (2005). Five psychometric scales for online measurement of the quality of human–computer interaction in web sites. *International Journal of Human–Computer Interaction*, *18*(3), 309–322.

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal internet use at work: Understanding cyber-slacking. *Computers in Human Behavior*, *27*(5), 1751–1759.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267–284.

Wenzel, M. (2004). The social side of sanctions: Personal and social norms as moderators of deterrence. *Law and Human Behavior*, *28* (5), 547–567.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston, MA: Thompson Course Technology.

Young, K. S., & Case, C. J. (2004). Internet abuse in the workplace: New trends in risk management. *Cyber-Psychology and Behavior*, *7*(1), 105–111.

About the Authors

Morgan M. Shepherd is a Professor of Information Systems at the University of Colorado–Colorado Springs. He received his PhD in Management Information Systems from the University of Arizona after having worked for over 10 years in the industry. His research interests include virtual groups, distance education, and security.

Roberto J. Mejias is an Assistant Professor of Computer Information Systems at Colorado State University–Pueblo. He received his PhD in Management Information Systems from the University of Arizona. He has 10 years of engineering experience with the IBM Corporation. His research interests include cyber security defense and cyber security risk management.