A Longitudinal Study to Determine Non-Technical Deterrence Effects of Severity and Communication of Internet Use Policy for Reducing Employee Internet Abuse

Morgan Shepherd
University of Colorado
@ Colorado Springs
mshepher@uccs.edu

Roberto Mejias
Colorado State University-Pueblo
roberto.mejias@colostate-pueblo.edu

Gary Klein
University of Colorado
@ Colorado Springs
gklein@uccs.edu

Abstract

This is the second part of a longitudinal study that examines how employee Internet abuse may be reduced by non-technical deterrence methods, specifically via IT acceptable use policies (AUP). Both studies used actual usage and audit logs (not self-reporting measures) to monitor the web activity of employees. In the earlier study, a mild AUP reminder to company employees resulted in a 12 percent decrease in non-work Internet usage. The current study utilized a more severe AUP communication and resulted in a 33 percent decrease in non-work Internet usage. For both studies, the AUP reminder resulted in an immediate decrease in non-work Internet usage. Results indicate that while non-work traffic under both treatments returned over time, the longevity effect of the severe AUP message was greater than the mild AUP message and non-work traffic did not return to its previous pre-treatment level by the end of the study.

1.0 Introduction

The abuse of technology in the workplace continues to be a major concern for organizations. Technology abuse can take many forms such as breaches of restricted IT resources, policy violations, piracy of copyrighted material and employee internet abuse. Internet abuse, often termed "cyber loafing", involves various non-work related Internet activities such as online chatting, personal emails, downloading music, blogging, instant messaging, stock trading, online gambling and even various forms of pornography and cybercrime. It is estimated that eighty percent of employees use the Internet during work hours for personal purposes [18a, 26], creating a discernible loss of productivity for both employees and organizations [9], [11]. Internet abuse as cyber loafing ties up bandwidth and degrades system performance [27] and may increase the legal liability for companies in the way of harassment, copyright infringement, intellectual property theft and the downloading of unlicensed software [4], [11], [33].

Internet abuse has shown a high correlation to the introduction of viruses, Trojan horses, spamware, rootkits and a host of other cyber-threats that compromises the integrity of information systems and facilitates unauthorized breaches of intellectual property and data [16]. In many cases employees do not perceive the personal use of the Internet as wrong and are quick to justify their actions [9], [25]. Maintaining the integrity of information system security is considered to be a top priority by organizations and a significant amount of research has investigated the relationship between I.S. security and employee work behavior [3],[4],[5],[26],[29]. Subsequently, there has been increased attention focused on employee workplace behavior, compliance with Internet use policies and the abuse of IT resources and how this affects IS security [28]. While it may not be clear as to where the pendulum swings along the "beneficial use vs. abuse" continuum regarding the Internet, it is reasonable to assume that employee Internet abuse is detrimental to organizations on many levels [25].

Organizations, in their attempt to reduce security breaches and reductions to employee productivity have sought to decrease employee internet abuse by monitoring, surveillance, personal penalties and the enforcement of technology acceptable use policies. Interestingly, a majority of employees themselves believe that personal email and internet use decreased their productivity [20]. Given the potential security impact and productivity loss of Internet abuse it is important to research methods to manage Internet abuse, particularly cyber loafing in an effort to reduce its occurrence and minimize its negative outcomes [6], [11], [15], [29].

The current paper incorporates a two-part longitudinal study that examines how employee Internet abuse may be deterred or reduced by non-technical deterrence methods, specifically via IT AUP. The first study utilized a mild AUP reminder to users that company's IT resources were to be used for business purposes only. The current study, conducted one year later and using the same employee pool

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.392

utilized a more severe communication of the AUP along with specific sanctions for user non-compliance to determine if it would deter or reduce employee Internet abuse. The remainder of this paper discusses prior research as a theoretical framework, our research model and hypotheses, research methodology, results, discussion, limitations and conclusion.

2.0 Prior Research and Theoretical Framework

Numerous researchers state that compliance with formal AUP, with regard to Internet use, are frequently employed as a form of security by raising user awareness to the dangers of internet abuse [11], [19], [29], [33]. Since employees who comply with the information security rules and policies are the key to strengthening information security, understanding compliance behavior is crucial for organizations wishing to leverage their human capital [3]. Underlying the need to reduce internet technology abuse has been the concept of *deterrence*.

Deterrence has been defined as the use of punishment or consequences as formal sanctions to deter individuals from committing some prohibited, restricted or illicit activity [4], [5], [31]. There are two key assumptions related to 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 punishment will prevent others from committing similar crimes [4], [5].

Deterrence countermeasures may refer to both technical and non-technical measures. Technical countermeasures refer to access control, strong passwords, firewalls, anti-virus software, encryption, intrusion detection systems, and honeynets to name a few [18], [32]. Non-technical countermeasures refers to information security policy (ISP), information and education (SETA), and contingency planning that guide employees in the acceptable use of systems and compliance with acceptable Internet use policies. Non-technical remedies also refer to legal action such as prosecution, incarceration, fines and termination. While technical deterrence technologies such as keystroke loggers, audit logs and video monitoring are often employed to reduce personal abuse of the Internet, research studies have shown that workplace satisfaction decreases when these types of deterrence countermeasure are used [25].

Within this context we considered previous I.S. research and related theories to understand how deterrence may reduce or prevent undesired internet abuse. There are a number of theory-based empirical studies on information security policy compliance by employees, suggesting that this area of research is becoming increasingly important [4], [10]. Much of the prior research in general deterrence theory (GDT) focuses on fear-based mechanisms, formal sanctions and threats to information organization's security [5]. However, D'Arcy and Herath point out that despite its solid foundation in criminology and its empirical support predicting illicit behavior within organization settings [21], [24] GDT may not fully explain IT and Internet abuse. Additionally, D'Arcy and Devaraj [4] state that while extant research affirms the deterrent effectiveness of sanctions, a substantial variance remains in many studies indicating that classical deterrence theory alone may not provide a complete understanding of technology misuse. Subsequently for the current study we found several theoretical frameworks that would complement GDT in understanding Internet abuse and deterrence. Our research found that *General Deterrence Theory (GDT)* [1], [5], *Agency theory* [6], [12], and *Rational Choice Behavior (RCB) theory* [2], [4], also provided relevant theoretical frameworks for the current study in understanding technology abuse and deterring Internet abuse in particular.

All three theories possessed components that considered penalties, and consequences for non-compliance behavior in the workplace. Since GDT is based in part on many of the precepts of RCB, there were several areas of communality that proved insightful in understanding Internet abuse and deterrence. Both GDT and RCB provided similar components that considered the severity of the deterrent (e.g. cost or penalty) against the illicit behavior and the expectations of such cost or penalty being enacted. Agency theory complimented this commonality with GDT and RCB by seeking to explain "compliance" in relation to penalties for incongruent organizational behavior. All three theories sought to understand appropriate behavior and provide incentives to encourage appropriate workplace behavior.

2.1 Rational Choice Behavior (RCB) Theory

RCB suggests that potential offenders consider the related costs and benefits in deciding whether to commit a particular deviant or illicit act [2], [5]. RCB theory has two basic assumptions: (1) that decisions to commit an illicit act consider both the costs (i.e., penalties) and benefits of the act, and (2) that this decision is affected by decision maker's perceived *expectations* of the related benefits and cost of that act [16]. Employees are likely to abuse Internet access if the related risks can be justified by the perceived benefits of the Internet abuses.

RCB theory has been adapted to various 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 [16], [21]. Since users are the weakest link in information systems, deviant behavior by individual employees generate the biggest impact on the security of an organization by visiting non-work related websites and downloading non-work related software [16]. In this context, individual employee assessment of the costs and benefits of deviant behavior (Internet abuse) are critical determinants of compliance with their organizational AUP.

2.2 General Deterrence Theory (GDT)

Classical deterrence theory focuses on formal or legal sanctions and proposes that the greater the perceived certainty, severity and swiftness of sanctions imposed upon an individual for an illegal or illicit act, the more individuals are deterred from committing that act [5], [7]. Contemporary deterrence theory is based upon the "rational choice" view of human behavior and that individuals weigh the perceived risks and costs of both formal and informal sanctions in deciding whether or not to engage in an unauthorized or illicit activity [5], [24]. Deterrence theory is one of the most widely applied theories related to behavioral IS studies and provides a prominent theoretical perspective in the area of employee Internet abuse [5]. Research has used deterrence theory as a foundation to predict user behavior in the workplace that is supportive or non-compliant with the organizational AUP particularly with regard to I.S. security. Interestingly, D'Arcy and Herath point out that despite its solid foundation in criminology and its empirical support predicting illicit behavior within organization settings deterrence theory may not fully explain IT and Internet abuse [5], [21], [24].

2.3 Agency Theory

Eisenhardt and Jensen and Meckling [6], [12] offers insights into information systems, outcome uncertainty, incentives and risk as related to organizational environments. The most common form of agency theory is when the owner of resources (principal) hires or employs another party (agent) to perform some prescribed work or task. When such an agreement is made through a contract the lack of perfect or complete information about intended goals and productivity between the principal and the agent may lead to information asymmetry and goal incongruence [6], [8]**.** Specifically, the goal(s) of the agent may be inconsistent with the goal(s) of the principal.

Internet abuse may be an example of goal incongruence in the principal-agent relationship of Agency theory where an employee (agent) is using the principal's resources for cyber loafing which is in conflict to the productivity and best interests of the employer (agent). Several methods to address this agency problem (i.e., Internet abuse) include monitoring Internet activities, logging which web sites agents have visited and developing white (appropriate) and black (non-work or inappropriate) websites [6], [8], [10], [11].

Agency theory contributes to our understanding of the need to address cyber loafing to verify appropriate behavior in the workplace and deter IT and Internet abuse. Agency theory has also been used to explain compliance with information security policies with regard to penalties, the social pressure of fellow workers, and the perceived effectiveness of one's security behaviors [10].

3.0 Research Model and Hypotheses

While information security planning and policy involves the implementation of technical and non-technical controls, non-technical deterrence measures have been shown to be more effective in safeguarding IT assets and preventing IT asset abuse [9], [23]. Most organizations employ SETA programs, information security policies and acceptable use policies (AUP) detailing what constitutes acceptable usage of IT resources to reduce various types of non-work activities. Internet use policies and related sanctions are considered to be the first line of intervention or deterrence in helping employees become mindful of the ethical use of company equipment [15]. Our current study focuses on the effect of *reminders* of AUP (acceptable use policy) monitoring, the *severity* of the (AUP) message, and the *longevity effect* of the AUP message as depicted in Figure 1.

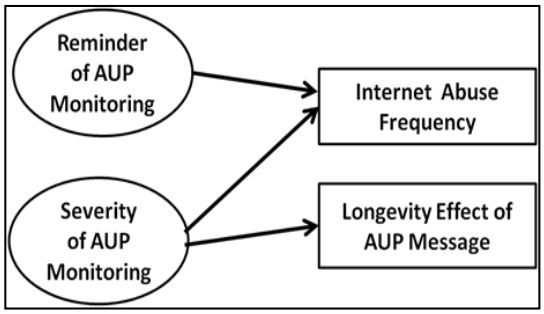

Figure 1. General Research Model

3.1 User Reminders of AUP Monitoring

Monitoring and surveillance of Internet usage by employees has been found to be an effective deterrent to decreasing internet abuse [10], [11], [13]. While some research indicates that organizational polices regarding Internet abuse are not likely to improve ethical behavior, numerous studies indicate that AUP policies and sanctions generate an impact upon user behavior and ethical conduct [5], [15], [29]. Additional studies demonstrate that obliging employees to simply sign an AUP will not reduce internet abuse [7], [8], [17] but that aggressive ISA (information security awareness) programs that remind employees of formal sanctions may affect employee internet abuse [10], [11]. The role of formal sanctions has been widely researched using deterrence theory and has been suggested as the primary mechanism for reducing computer abuses [4], [5]. Rational choice theory also affirms formal sanctions as important instruments for deterring deviant behaviors [16]. Deterrence mechanisms consist of two dimensions: detection probability (or sanction certainty) and sanction severity [21], [31]. Both dimensions are related to an individual's *perception* of the probability they will be "caught" abusing Internet privileges rather than the actual *detection* probability and sanction severity level.

Deterrence theory also assumes that potential violators are made aware of efforts (e.g., AUP reminders) to control anti-social behaviors [22]. However, even if employees are not fully aware of the contents of their organization's Internet use policies, deterrence theory suggests that policies, like laws may be effective when the content is *communicated* to users [22]. Agency theory suggests that lack of perfect information between the principal (i.e., the organization) and the agent (i.e., the employee) often results in information asymmetry regarding the use of organizational resources (i.e., Internet) for cyber-loafing [8]. If employees are aware of ongoing monitoring and detection efforts, they are more likely to obey the policies [4], [10]. With higher awareness created by reminding employees that existing detection mechanisms are in place, employees may be more likely to comply with the security policies. Therefore, we propose:

> H1: Repeated *reminders* to Internet users of the organization's AUP will reduce Internet abuse.

3.2 Severity of AUP Message

There has been considerable research regarding the role of sanctions and the severity of penalties in exerting deterrent effects on deviant acts. A review of the related literature on deterrence suggests that as the level of punishment (i.e. severity) increases, an individual may be less inclined to carry out a particular deviant act [4], [10]. Similar logic can also be applied to the use of company IT resources where employees non-adherence to security policies can be deterred by imposing high levels of penalties or other disciplinary actions [4], [10].

According to rational choice behavior theory, the perceived *severity* of a sanction may be an important influence in deterring unwanted or deviant behavior [4]. High levels of perceived severity of sanctions increases the perceived *cost* of deviant behaviors and may counteract the attractiveness or perceived benefit of a deviant behavior [5]. Based upon these findings we hypothesize that employee internet abuse will reduce in frequency in direct proportion to the severity of the Internet abuse policy message. Therefore, it would be reasonable to expect that a more severe AUP message with related sanctions would increase the perceived cost (i.e. penalty) of Internet abuse. Therefore, we anticipate that:

> H2: Internet abuse frequency will decrease as the *severity* of the AUP message increases.

3.3 Longevity Effect of AUP Message

Rational Choice Behavior and GDT posit that the greater the perceived severity of sanctions (i.e., cost of the penalty) for an illicit act the more individuals are deterred from committing that act [4], [7]. The severity of organizational Internet use policies may also have a mitigating effect on the longevity of Internet abuse [8], [14], [19], [30]. Security and Internet use policies usually contain statements of organization mission, goals, policies and employee responsibilities with specific guidelines regarding the use of organizational IT resources. Information Security Awareness (ISA) programs seek to increase employee awareness of the dangers of cyber-threats and their responsibility in using organization IT resources for business purposes only [18]. It would therefore be reasonable to assume that a more severe AUP message to users of the consequences and penalties for non-compliance would have a longer effect (i.e., longevity) on the frequency of Internet abuse than a mild AUP message. Therefore, we hypothesize that,

> H3: A *severe* AUP message reminder will generate a *longer* effect in reducing the frequency of internet abuse than a *mild* AUP message.

4.0 Research Methodology

Much of extant research on Internet abuse has focused on short term studies to determine if users responded to a particular experimental treatment [8]. Early studies on the effectiveness of formal security policy as a deterrent to reduce Internet abuse found inconsistent results [5]. Additionally, much of the prior research on using security policy as a deterrent to reduce Internet abuse relied upon self-reported surveys. The current study and previous study utilized actual user data and aggregate audit logs to analyze the effect of non-technical deterrence measures to reduce Internet abuse. For the previous study a one-time screen message from the organization's IT department gently reminded users of the AUPs that they previously signed. The pop-up screen was a mild AUP reminder that company's IT resources were to be used for business purposes only. The current research study utilized a one-time but more severe AUP message (along with related sanctions) than the previous study to determine if a stronger non-technical deterrent would generate a greater reduction in employee internet abuse.

The current research study uses two longitudinal time frames exactly one year apart. Our first study [25] utilized 200 employees from the areas of accounting, finance and human resources from a single organization. The same employee pool of 200 employees was used for the second study with only minor changes in personnel. For both studies the agreement we had with the organization was that in order to collect data the identity of our organization and its related industry had to be kept confidential. We are allowed to say that the employees in our sample are all working professionals. The company is a SMB located in the mid-western United States. All employees were required to take company provided SETA (security education) training, which was offered in the form of an online training program and follow-up quiz. Procurement of the field research data was problematic and time consuming, however, as researchers were required to provide assurances that web traffic monitoring and Internet activity would not be tracked to individual users.

Our experiment used *Splunk*©, a log monitoring and data reporting search tool for analyzing the web activity of the IP addresses from our sample user group. All individual IP addresses were static throughout the research study. Web traffic was monitored during the first week to establish a baseline level of activity. The experimental treatment, in the form of a one-time pop-up AUP message was sent to all 200 subjects as well as the company's IT department. The less severe or "mild" experimental script from the first study used the following AUP message:

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

For the current study the experimental script was more severe with an additional reminder of the related sanctions or penalties for non-compliance:

> "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."

For Study 1 (mild AUP) and study 2 (severe AUP), the experimental treatment was introduced only once at the beginning of the study and not repeated for any subsequent data collections. The company's IT group activated the Splunk© software and collected all internet traffic data from the subject pool. The Splunk© software ran for approximately five weeks, 24 hours each day. Data collection started about one week before the treatment and continued for a few weeks after the treatment. We sent out the AUP reminders (as the experiment treatment) on Tuesday, and allowed two days for the message to be viewed by all employees in our subject pool. The first data reading (D1) was analyzed on Thursday, two days after the AUP reminder. To minimize any day-of-the-week confounds and to maintain data collection consistency related to a particular week day, we used the data from the previous Thursday before the experimental treatment as our pre-treatment benchmark. We then analyzed data from the subsequent Thursdays for our study's data readings (D1, D2, D3).

Additionally, to control for the confounding effects of whether employees were visiting non-work related websites during their lunch hour (approx, 12:00 pm to 1:00 pm), only web traffic data collected during the hours of 9:00am to 11:00am was analyzed. This experimental control was to confine our analysis of Internet web surfing behavior data to standard work hours. A two hour span provided more than enough data to analyze. While a different two hour window (1:00 - 3:00 pm or 2:00 - 4:00) could have been used the researchers felt that the morning window would provide the least amount of non-work Internet usage and would provide a more conservative result. Of note is that there were no major events occurring within the company or in the media during the study. As we collected data at the aggregate level, individual

source IP addresses were not known to assure employee privacy and confidentiality.

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

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 network, web, search engine and server traffic
4. Tunes	Online music sites
5. Non-work	Non-business related sites

Table 1: Category descriptions

While social networks are frequently used by company HR to review potential job candidates, inclusion of these websites may have had the potential to skew the results from the non-work category. Category 3 (Neutral) referred to all network traffic generated by web surfing in general, such as server hits, marketing ads and search engine traffic. As this type of web traffic is generic to all web surfing, these particular web sites were categorized as neutral. Category 4 (Tunes) referred to online music websites and constituted a very small percentage of overall web traffic (< 3%). Category 5 (non-work) consisted of all website traffic that was not directly or indirectly business related. Some examples would be .mlb (major league baseball), department stores, recipes, style and fashion sites, Hollywood gossip sites and online shopping sites (see Table 1).

5.0 Results

The number of websites visited over the two hour experimental period for each experimental date was approximately 55,000 websites for Study 1 and approximately 45,000 websites for Study 2. For both studies the network component of Category 3 ("Neutral") constituted the majority of the website counts. As our research study was intended to focus only on work-related (Category 1 "Business-related") and Internet abuse related websites (Category 5 "non-work") we removed the Category 2 ("Mixed"), Category 3 ("Neutral") and Category 4 ("Tunes") data from our current analysis. The results from both studies are shown in Table 3 and Table 4 respectively. "Count" refers to the number of web visits for a particular category and "%" refers to the relative percentage of that category count to the total count of Business-related and non-work websites visited over the experimental two hour periods. For consistency, we utilized the % column as the aggregate number of web traffic differed between the two studies.

Table 2 shows a summary of Chi-square test of distributions and the results of hypothesis testing:

	H1	H2	H3
Chi Sq.	1030	267	27
p	< .05	< .05	< .05
Supports Hypothesis?	Yes	Yes	Yes

Table 2: Study #2 (Severe AUP Message)

In both studies the experimental treatment was a pop-up screen reminder to employees to adhere to the company's AUP. Study #1 used a mild or less severe reminder of the company AUP policy. Study #2 used a more severe reminder of the AUP policy with a reminder of the related sanctions or penalties that would be imposed for user non-compliance. A Chi-square test of distributions of the Business-related vs. non-work related websites traffic indicated that the differences in distributions from the pre-experiment treatment to the post-experimental treatments were each significantly different at the $p < 0.05$ level (see Tables 3 and 4 for the counts and percentages).

Results from the first study (Table 3) indicate that the amount of non-work web traffic decreased from 55% to 43%. Results from the second study (Table 4) which used a more serious AUP reminder indicated a greater and more significant decrease in non-work website traffic from 72% to 39%. A test of proportions also indicated that the percentage of business-related website visits for both studies increased with the proportion of non-work visits decreasing after the introduction of the AUP message post-treatments, significant at $p < .05$.

	Pre-Treatment		Post-Treatment	
Category	Count	%	Count	%
Business	8132	45	9563	57
Non-work	9766	55	7107	43
Totals	17,898		16,670	

Table 3: Study #1 (Mild AUP Message)

Table 5 displays the results generated from Study #1 with data collected over 3 time periods: one pre-treatment and two post-treatment readings (D1, D2). D1 was the data collected two days after the treatment, and D2 was the data collected one week after D1.

Category	Pre-Treatment		Post-Treatment	
	Count	%	Count	%
Business	4849	28	1613	61
Non-work	12246	72	1041	39
Totals	17,095		2,654	

Table 4: Study #2 (Severe AUP Message)

Table 5 indicates that the count for the percentage of non-work website traffic is relatively high (55%) before the introduction of the AUP pop-up message. For post-treatment reading D1, non-work website traffic decreased by 12% to 43%. However, the Non-work web traffic level at post-treatment reading D2 (60%) had returned to its approximate Pre-Treatment level (55%).

Category	Pre-Treatm't	D1 Read'g	D2 Read'g
Business	45%	57%	40%
Non-work	55%	43%	60%

Table 5: Study #1 (Mild AUP Message)

Table 6 displays the percentage results generated from Study #2. All previous experimental conditions were replicated and all Internet web traffic measures were again taken on the same work weekday (Thursday). As before, D1 was the data collected two days after the treatment, and D2 was the data collected one week after D1. D3 was the data collected one week after D2 (two weeks after D1). Table 6 indicates that the percentage for non-work website traffic was relatively high at 72% but decreased significantly ($p < .05$) to 39% after the introduction of the severe AUP message. The percentage of Non-work website traffic gradually increased to 50% and 59% respectively for post-treatment readings (D2, D3). However, the percentage of non-work website traffic at D3 (59%) remained lower than the initial pre-treatment level (72%). So two weeks after the treatment, non-work website traffic was still below pre-treatment levels.

Category	Pre-Treatm't	D1 Read'g	D2 Read'g	D3 Read'g
Business	28%	61%	50%	41%
Non-work	72%	39%	50%	59%

Table 6: Study #2 (Severe AUP Message)

6.0 Discussion

Our results indicate interesting findings with respect to the effect of non-technical deterrence measures in the form of AUP reminders to employees. Hypothesis 1 (*Repeated reminders to Internet users of the organization's AUP will reduce Internet abuse*) was supported by the results. For Study #1 (mild AUP) the percentage of non-work websites traffic decreased ($p < .05$) after the introduction of the AUP reminder. However, this reduction effect for non-work website traffic was not sustained for the post-treatment reading D2. At D2, the percentage of non-work websites traffic (60%) returned to its approximate Pre-Treatment level of 55%.

Study #2 (severe AUP) generated similar results one year later with an additional post-treatment measurement (D3), taken approximately three weeks after the introduction of the experimental treatment. Specifically, Study #2 generated a larger and more significant decrease in non-work website traffic from 72% to 39% at the D1 reading. Subsequent readings for D2 and D3 however, displayed a gradual increase in non-work website traffic. However, non-work website traffic levels D2 and D3 were still lower than pre-treatment levels two weeks after the treatment.

These results may be partially explained by several factors. The initial introduction of any Internet usage policy reminder to users may have generated a renewed awareness that Internet use policies were now being monitored by the organization. However, after the initial awareness was established and non-work web traffic decreased for both studies at the post-treatment readings D1, the "novel" effect of the AUP message may have been attenuated since AUP "reminders" were not employed again at subsequent post experimental readings. Subsequently, non-work web traffic levels started to gradually return towards their initial pre-treatment levels for both Study #1 and #2. Agency theory may be used to explain that the absence of AUP reminders to users may have contributed to the lack of perfect information about intended goals and productivity between the principal (the organization) and the agent (Internet user) generating information asymmetry and goal incongruence. Additionally, no consequences or penalties for violating the company's AUP were reported to employees which may also have contributed to the attenuation effects of the AUP message after D1.

For Study #1, rational choice behavior could be used to explain the quick return to pre-treatment non-work related web traffic levels. Since the mild AUP message did not mention any related sanctions or penalties for non-compliance, employees may have

perceived that a low cost and higher benefit could be derived by visiting non-work websites and violating the AUP. Deterrence theory proposes that since instances of perceived certainty, severity, and swiftness of sanctions imposed for an illicit act were not clearly communicated, employees may have been less deterred by the mild AUP reminders. For Study #2, the lower upsurge in the percentage of non-work web traffic for D2 and D3 could be explained by deterrence theory. Specifically, the more severe AUP message that sanctions and penalties would be imposed upon violators may have generated more profound and sustained effect upon users for Study #2 such that non-work traffic levels for D2 and D3 had not reached Pre-treatment levels as observed for Study #1.

Hypothesis 2 (*Internet abuse frequency will decrease in proportion as the severity of the Internet abuse policy message increases*) was supported as illustrated in Figure 2. Figure 2 clearly contrasts the effects of the two experimental AUP treatments (Mild vs. Severe). As depicted in Table 6, even though Study #2 started with higher pre-treatment levels of non-Work website traffic (72%) than Study #1 (55%), the effect of a more severe AUP message with related penalties and sanctions generated a significantly ($p < .05$) greater decrease in non-work website traffic than the mild AUP message from Study #1. The severe AUP message also generated a more sustaining effect than Study #1 by keeping non-work web traffic below its Study #2 pre-experiment treatment levels for a longer period of time. Additionally, non-work web traffic levels for the severe AUP message did not approach the same proximity in percentage as did the mild AUP message used for Study #1.

The more severe AUP message may have affected the rational choice decision of potential Internet abusers. Specifically, rational choice behavior theory posits that a cost benefit analysis is undertaken by employees contemplating an illicit act. The stated costs and penalties associated with the more severe AUP treatment could have dissuaded potential abusers from visiting non-work websites more than the mild AUP treatment message from Study #1 which did not mention sanctions or penalties. General Deterrence theory may also be used to partially explain the larger decrease in non-Work traffic generated by the more severe AUP message. Specifically, the more severe AUP message that sanctions would be imposed upon violators may have dissuaded employees from the perceived certainty that penalties would be imposed if such deviant behavior continued.

Our results support Hypothesis 3 *(A severe AUP message reminder will generate a longer effect in reducing the frequency of internet abuse than a mild AUP message.)* For Study #1 the initial introduction of a AUP reminder message (albeit mild) on user screens was influential enough to initially reduce non-work website traffic. However, as seen in Figure 2, this effect was not sustained for D2 for Study #1. In contrast, Study #2 which used a more severe AUP message (along with stated sanctions for non-compliance), maintained lower percentage levels overall of non-work website traffic than Study 1 which used a mild AUP message. The percentage of non-work website traffic also remained below its pre-experimental levels for D1, D2 and D3.

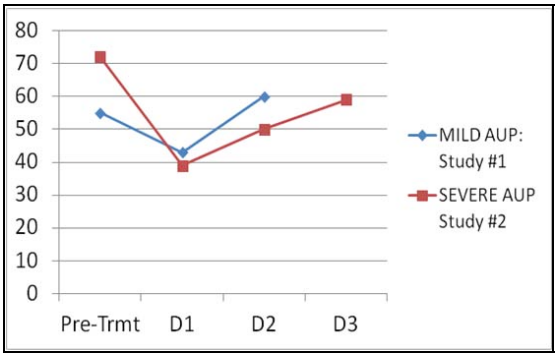

Figure 2: Non-work Traffic: Mild vs. Severe AUP

Rational choice behavior theory and deterrence theory may be used to partially explain these results. Not only did the costs and penalties associated with the more severe AUP message dissuade potential abusers from visiting non-work websites but the sustaining effect of the more severe AUP may have been convincing enough to *continue* to maintain non-work web traffic levels lower than the mild AUP message treatment. While it may be argued that such a comparison of Study #1 and #2 had different numbers of non-work website traffic data points an extrapolation of the trajectory of the mild AUP graph line could be assumed to continue above the severe AUP graph line.

6.1 Limitations of the Findings

While the management of the organization in our study assured us that virtually the same employee pool was used for both Study #1 and #2 (which were taken 1 year apart), our first limitation is that minor attrition or employee turnover may have generated a small effect upon the results. However, we believe that this effect would be minimal given that workplace Internet practices are somewhat common and widespread across many population samples [17]. Our second limitation refers to finding an accepted standard or methodology for categorizing which Internet sites should be classified as "business" or "non-work"

related as our results could be affected by our categorization of the social networking websites. To reduce the effects of this confound we incorporated a conservative approach in our methodology and did not include data from the "non-work" category for the reasons previously cited. Our third limitation refers to the nature of the severe AUP experimental treatment. The combination of a more severe AUP message together with a warning of sanctions and penalties for user non-compliance may have generated a confound effect which could have influenced the final percentage results. However, removing the warning of sanctions and penalties component of the severe AUP treatment would not have differentiated it substantially from the mild AUP message to justify Study #2. Finally, our fourth limitation refers to the generalizability of our findings. Since our study was exploratory in nature, we used the same employees from the same organization thus limiting our findings to a larger industry segment or population. The authors intend to incorporate more subjects from different organizations in a future paper. Despite these limitations we believe that the results generated by the more severe experimental treatment for Study #2 generates interesting implications for the support of using a more severe reminder of the organization AUP and penalties for non-compliance.

7.0 Conclusion

The results of this study generated interesting findings and implications for researchers and practitioners. Our results suggest that non-technical deterrence methods in the form of Internet use policy reminders may constitute an effective approach to reducing employee technology abuse particularly with regard to workplace Internet abuse. For our analysis, employees were exposed to both a mild (Study #1) and severe (Study #2) version of the organization's IT AUP. For both treatments the introduction of a one-time reminder of the AUP generated an immediate decrease in the percentage of non-work website traffic. The more severe AUP treatment which also included stated penalties for user non-compliance reduced non-work website traffic percentage levels that were significantly lower than the mild AUP treatment.

However, for both studies the effect of reducing non-work websites traffic was not sustained over time. Specifically, for the mild AUP message treatment the percentage of non-work Internet traffic gradually increased and returned to its previous pre-treatment levels. For the severe AUP treatment, the percentage of non-work Internet traffic also gradually increased but remained significantly below its previous pre-treatment levels and significantly below the levels generated by the mild AUP treatment. Additionally, the longevity effect of the severe AUP message was greater over time than the mild AUP message.

Since both the mild and severe AUP treatments were each administered only once as a one-time message at the beginning of each study, it would be reasonable to imply that their respective effects could have been attenuated since "reminders" of the company's Internet use policies were not communicated to employees. When AUP rules, policies, and regulations are not regularly communicated into the normal business routine of an organization, user Internet abuse may continue or increase. This implies non-technical deterrence measures that request compliance to Internet use policies must be periodically communicated to employees to remain effective. As employee internet abuse in the form of lost man-hours and related productivity constitutes a significant expense for organizations the authors encourage more research in the area on non-technical deterrence measures to reduce employee technology abuse.

8. References

[1] Beccaria C. (1963) Essays On Crimes and Punishment. New York: Macmillan,

[2] Becker, G.S. (1974) Essays in the Economics of Crime and Punishment, Columbia University Press

[3] Bulgurcu, B., Cavusoglu, H., & Benbasat, I (2010). Information Security Policy Compliance: An empirical study of Rationality-Based beliefs and information system awareness, *MIS Quarterly*, *Vol. 34 (3),* 523-548.

[4] D'Arcy J. & Devaraj, S. (2012). Employee misuse of Information Technology Resources: Testing a contemporary deterrence model, *Decision Sciences, Vol. 43 (6),* 1091-1124.

[5] 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*, *Vol. 20 (6),* 643–658.

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

[7] Gibbs, JP. (1975) Crime, Punishment, and Deterrence. New York; Elsevier

[8] Glassman, J., Prosch, M., & Shao,B. (2013). **"**Active Real Time Internet Usage Warnings: A Countermeasure For Cyberloafing.", *12th Annual Security Conf.,* Las Vegas, NV.

[9] Goulder, M.H. (2011). *Network Defense: Security and Vulnerability Assessment. Course Technology*, Cengage Learning, EC-Council Press, Volume 5 of 5.

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

[11] Henle, C. A., Kohut, G., & Booth, R. (2009). Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing. *Computers in Human Behavior*, *Vol. 2 (4),* 902 – 910.

[12] Jensen, M. L., & Meckling, W. H. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. *Journal of Financial Economics, Vol.3 (4)*, 305-360.

[13] Jessup, L. & Urbaczewski (2002). "Does electronic monitoring of employee internet usage work?" *Communications of the ACM*, *Vol. 45 (1)*, 80-83.

[14] Johnson, J, & Ugray, Zsolt. (2007). "Employee Internet Abuse: Policy Versus Reality," *Issues in Information Systems*, *Vol. 8 (2*), 214-219.

[15] Kolkowska E. & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, *Vol. 33*, 3-11.

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

[17] Martin, L. Internet use, innovative workplace practices and workers' motivations: Empirical evidence at the European level. (2012) *61ème Colloque de l'Association Française de Science Économique (AFSE)*, Paris : France

[18] Mejias, R.J. (2012) An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk Proceedings of the *45th Hawaii International Conference on Systems Sciences (HICSS).*

[19] 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*, Vol. 2 (3-4), 302-324.

[20] Muhl, C.J. (2003)Workplace email and Internet use: Employees and Employers beware. Monthly Labor Review, February. 38-44.

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

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

[23] 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*, *Vol. 25 (2)*, 125–144

[24] 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 Taking Stock: Status of Criminological Theory, New Brunswick, NJ. *Transaction Publishers*, 37–76,

[25] Shepherd, M. & Klein, G.. (2012). Using Deterrence to Mitigate Employee Internet Abuse. Proceedings of the 44th Annual *Hawaii International Conference on Systems Sciences* (HICSS), Waikola Hawaii,

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

[27] Sipior, J.C. & Burke T.W. (2002). A Strategic Response to the Broad Spectrum of Internet Abuse. *Information Systems Management*, *Vol. 19 (4),* 71-79, 2002

[28] Warkentin M. & Willison R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, Vol. 18 (2),* 101–105.

[29] 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, Vol. 20 (3),* 267-284.

[30] Weaver, K. M. & Ferrell, O.C. (1977). The Impact of Corporate Policy on reported ethical beliefs and behaviour of marketing practitioners. in B. A. Greensburg and D. N. Bellenger (eds.), *Contemporary Marketing Thought '77. Educators' Proceedings,* No. 41 (American Marketing Association, Chicago), 477–481.

[31] Wenzel, M. (2004). The social side of sanctions: personal and social norms as moderators of deterrence. *Law and Human Behavior, Vol. 28 (5),* 547-567.

[32] Whitman M.E. & Mattord. H.J. (2012) *Principles of Information Security*, 4th Edition. Boston MA: Thompson Course Technology.

[33] Young, K.S. & Case, C.J. (2004). Internet Abuse in the Workplace - New Trends in Risk Management. *Cyber-Psychology and Behavior*, *Vol. 7(1)*, 105-11