Using Deterrence to Mitigate Employee Internet Abuse

Morgan M. Shepherd  
Business Analysis Department  
College of Business  
University of Colorado at Colorado Springs  
1420 Austin Bluffs Parkway  
Colorado Springs, CO 80918  
mshepher@uccs.edu

Gary Klein  
Business Analysis Department  
College of Business  
University of Colorado at Colorado Springs  
1420 Austin Bluffs Parkway  
Colorado Springs, CO 80918  
gklein@uccs.edu

Abstract

This study looks at the question of how to reduce/eliminate employee Internet Abuse. Ethics play a large role when it comes to personal use of company resources during the workday. Companies are trying to reduce/eliminate this personal use during the workday in an effort to cut down on productivity losses and excess bandwidth use. Companies have used acceptable use policies (AUP) and technology in an attempt to mitigate employees’ personal use of company resources. Research shows that AUPs do not do a good job at this but that technology does. Research also shows that while technology can be used to greatly restrict personal use of the internet in the workplace, employee satisfaction with the workplace suffers when this is done.

While many of the previous studies have relied on self-reporting by the subjects, we monitored the usage logs of our subjects and used the actual web activity in this research. In this research experiment we used technology not to restrict employee use of company resources for personal use, but to make the employees more aware of the current Acceptable Use Policy, and measured the decrease in employee internet abuse. The results show that this method can result in a drop from 27 to 21 percent personal use of the company networks.

1. Introduction

The Internet and the WWW have become standard tools in the workplace, and are used by many organizations as the predominant way of doing business. However, there are also productivity losses associated with personal use of the Internet and WWW by employees during working hours. These stem from employees using the WWW and Internet for mundane things such as paying bills online to gambling and surfing pornography sites [2], [6], [11]. In some cases the employees do not see their non-work usage as wrong, and actually justify their actions [10].

The research in the area of internet abuse is not conclusive, however. While many studies have shown that there is indeed a loss of productivity, others suggest that there may be an acceptable amount of personal internet use by employees. These latter studies claim that employees’ personal use of the internet takes the place of interacting with co-workers at the water cooler, and may take less time. This personal use has also been found to help employees improve their job skills, reduce computer fear, and make the workplace more enjoyable [23], [1], [18], [15].

While it may not be clear as to where the pendulum swings along the ‘beneficial use vs. abuse’ continuum for each organization, it stands to reason that internet abuse can be detrimental to the organization. The purpose of this research study is to find a way to reduce the abuse without eliminating the beneficial use employees get from the personal use of the internet.

This research study is part of a larger effort of finding ways for corporations to effectively educate employees on the ethics of internet abuse, effectively educate employees on the cost of internet abuse, effectively mitigate employee internet abuse for the short term and effectively reduce or eliminate employee abuse for the long term. The specific aspect of this research study is to find an effective method to reduce employee internet abuse for the short term.
1.1 Corporate policies

Most organizations have security policies and acceptable use policies (AUP) that detail what constitutes acceptable usage of company equipment [19]. These are the first line of intervention in helping employees determine ethical use of company equipment. There isn’t a technology component involved with this so the costs involved with the creation of these are not that high. Employee education and ethics training are other non-technical means employers have to help employees determine proper usage of company systems.

1.2 Monitoring/restricting employee use via technology

Keystroke capturing is one technology that can be used in an effort to reduce personal use of the Internet by employees, and there are other technologies that can be used to monitor employee email, phone usage and IM. Video surveillance cameras can also be utilized in an attempt to see to the level of employee internet abuse. However, some research studies have shown that employee satisfaction with the workplace decreases when these are used [5], [7].

Firewalls represent another technology that can be used to restrict employee access to the internet. Most WWW traffic passes through port 80 on network routers. Most routers can restrict incoming/outgoing traffic over this port. While this can be utilized to greatly reduce internet abuse, it also curtails the benefits that the internet provides to businesses. Depending on the cost/functionality of the router, WWW traffic to specific sites can be restricted while allowing access to all other sites. However, the number of sites that would be considered ‘non-work’ sites may be too large to make this feasible.

Corporate policies such as Acceptable Use Policies are another means organizations employ to reduce internet abuse. While some research indicates that the use of codes of conduct is not likely to improve ethical behavior, Weaver and Ferrell indicate that these policies do have an impact on ethical conduct [24]. It has also been suggested that while the AUP may provide some improvement in employee behavior, it must be communicated to all employees. Simply having the employees read or sign an AUP without some type of refresher at periodic intervals will not reduce internet abuse [9], [8], [22].

Organizations are trying to find methods that will help employees reduce the amount of internet abuse without being intrusive in the workplace.

1.3 Deterrents and employee abuse

Webster’s defines ethics as “the discipline dealing with what is good and bad and with moral duty and obligation” and “the principles of conduct governing an individual or a group” [12]. Others have approached the definition from a specific discipline. In the technology arena, Moor wrote about ‘computer ethics’, saying “On my view, computer ethics is the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology.” [14]

Regardless of the specific definition, the academic study of ethics has been ongoing for the past few millennia. Some of the areas of study include the various definitions of ethics, how to best teach ethics and what influences people to behave ethically [21], [3], [17].

There are various opinions on how to teach ethics. From a business sense, Sims and Felton talk about four things to think about: the objectives or learning outcomes, the learning environment, the learning process and the roles of the participants [21].

Rest came up with a four stage model where “…the individual facing a decision with moral content first recognizes the moral issue, then makes a moral judgment, next establishes moral intent, and, finally, engages in moral behavior.” [17]. Based on his reviews of the research, Rest states that some type of intervention can be used to improve an individual’s moral development. While he does not prescribe a particular intervention, he does go on to say that some types are more effective than others – there is no silver bullet here.

In addition to ethics education, general deterrence theory may also shed some light on ways to lessen internet abuse. In general, this theory holds that strategies for managers to reduce the risk to systems come under four activities: deterrence, prevention, detection and remedies [4], [13]. Deterrence refers to education, policies and written guidelines that guide employees in the acceptable use of systems. Prevention refers to the common security practices of ID/password combinations, firewalls and door locks. Detection refers to key stroke capturing, video surveillance and user monitoring. Remedies refers to legal action such as punishment, termination and legal action. As you move from deterrence through remedies the cost to the company increases.

In their study on reducing internet abuse Mirchandani and Motwani looked at the effectiveness of deterrence, and found mixed results. However, their research relied on self reported results [13]. This current research study looks to see how well the AUP,
an example from the deterrence activity, can help reduce internet abuse.

2.0 Research Study

This research study was an attempt to find a way to reduce internet abuse in a fairly unobtrusive manner. It builds on the works of Rest and Weaver & Ferrell where an intervention in the form of a short message popping up on user screens reminds the users of the AUP, and asks them to think about the AUP before visiting websites. Due to the sensitive nature of this type of research, it took over eighteen months to get the necessary permissions to undertake this research. The CEO was not the main problem, although did account for six of the eighteen month delay. The primary holdout was the CIO, who had to be convinced that we would not track the web traffic back to any individual user.

After months of meetings with the CIO, the networking staff and the CSO (chief security officer) we were finally given permission to monitor the web traffic of a medium sized firm (approximately 2000 employees) over a three week period. One stipulation was that we are not allowed to acknowledge the company, or the industry they are in. We selected approximately 200 employees to monitor from the accounting, finance and human resources departments.

2.1 Research Methodology

The software program Splunk was used to monitor the web traffic from the range of IP addresses that made up the user group. These IP addresses were made static during the duration of the research study. Web traffic was monitored during the first week to establish a baseline. Then the treatment, in the form of a message from the IT department was pushed out to the screens of all the subjects. It asked the subjects to please consider the AUP and to only use the company systems for business purposes. The message took approximately three seconds to read and required the subjects to click to close it. A two day period was given to make sure the subjects had a chance to view the message. Web traffic was monitored during all that week and the next to see how well the treatment worked.

We waited for a three week stretch of time where it would be business as usual, and where there was not a major event going on within the company or in the media. For instance, we could not run the study during the World Cup soccer time period, the NCAA March Madness playoff or the Japanese quake events. We also could not run the study during certain times of the year when the company experiences non-traditional workloads.

The first week was used to collect the baseline data. At the start of the second week a short, three sentence message was sent to each employee. The message simply asked the employee to remember the AUP and to please use the company systems for business purposes only. Data was still being collected during this week, and continued through the third week of the study, even though no additional interventions were sent to the employees.

To lessen the confound of whether the employee was visiting non-work related websites during their lunch hour, only the Web traffic collected during the hours of 9:00am – 11:00am was analyzed. While not perfect this was an attempt to only analyze web surfing behavior data during standard work hours.

To help ensure consistent data was taken from the same day of the week to help eliminate that confound. Data was used from the Thursday of the baseline week, and from the following Thursday after the treatment was delivered to the employees.

Splunk broke out the web traffic into the various websites that were visited. A single visit to a web site generates multiple hits so the numbers at first appeared to be inflated. However this was consistent across all websites and all web traffic and it did not have any effect on the final percentages. This also has a tendency to incorporate an aspect of visits as well as time spent on a site.

We analyzed the traffic and broke it down into five major categories. The first category represented those sites that consisted of business use with a high probability. The majority of this traffic came from the company servers. While we could not see the actual screen shots that the employee used we were able to ascertain that the employee was at the accounting page of the corporate server, for example. These were put in the ‘business use’ category.

The second category represented mixed sites, those sites that might be work related but might not be. The large percentage of this category was social networking sites such as Facebook. While it would have made the numbers look much better had this category been included in the ‘non-work’ related category it was deemed better to err on the side of caution. This traffic was put in a category called ‘mixed’.
The third category was all the network traffic generated by web surfing in general, such as server hits, ads and search engine traffic. This is generic to all web surfing, and we put in a separate category called ‘neutral’.

The fourth category was all the online music site traffic. This was a very small percentage of the overall traffic (around 3%), but was still put in a separate category called ‘tunes’.

The fifth group was all the ‘non-work’ related traffic. Sites such as .mlb (major league baseball), department stores, recipes, style and fashion sites, Hollywood gossip sites and online shopping sites were included in here.

This is shown in table 1.0 below.

<table>
<thead>
<tr>
<th>Category</th>
<th>Brief explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>Site related to business activities</td>
</tr>
<tr>
<td>Mixed</td>
<td>Social networking sites – some of these might be business related</td>
</tr>
<tr>
<td>Neutral</td>
<td>Search engine and server hit generated traffic</td>
</tr>
<tr>
<td>Tunes</td>
<td>Online music sites</td>
</tr>
<tr>
<td>Waste</td>
<td>Not business related sites</td>
</tr>
</tbody>
</table>

Table 1

2.2 Hypothesis

From the works of Weaver and Ferrell [24] and Johnson and Ugray [9] it seems as if the organization’s policies can help reduce employee internet abuse. However, as the span from when the employee last reads the policy to the present day increases the effectiveness of the practice declines. Therefore, the hypothesis for this portion of the research project was that employee internet abuse will subside after the employees are reminded of the AUP and asked to utilize the company resources for business purposes only. That led to our hypothesis:

H1: Employee internet abuse will lessen after a non-intrusive reminder of the AUP.

3.0 Results

The usage values for the top 100 websites visited, accounting for approximately 2/3 of all traffic, are highlighted in Table 2. In both cases, the number of business plus waste sites total 50%. A Chi-square test of distributions indicates that the discrete distribution from one period to the next is significant at $p < 0.05$. A test of proportions also indicates that the percentage of business visits increased and the proportion of waste visits decreased from before to after the treatment. These results are, of course, extremely preliminary and will be supplemented with successive trials, though efforts were expended to select times and subjects that would yield minimal bias. The changes may be better seen graphically in Figures 1 and 2, before and after the AUP reminder.

<table>
<thead>
<tr>
<th>Category</th>
<th>Prior to treatment</th>
<th>After treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>count</td>
<td>%</td>
</tr>
<tr>
<td>Business</td>
<td>8132</td>
<td>23</td>
</tr>
<tr>
<td>Mixed</td>
<td>5153</td>
<td>14</td>
</tr>
<tr>
<td>Neutral</td>
<td>11945</td>
<td>33</td>
</tr>
<tr>
<td>Tunes</td>
<td>1079</td>
<td>3</td>
</tr>
<tr>
<td>Waste</td>
<td>9766</td>
<td>27</td>
</tr>
</tbody>
</table>

Table 2

4.0 Discussion

The results show that hypothesis 1 was confirmed at the .05 level, employee abuse of the internet lessened after the AUP reminder. It is important to note that these results are not self-reported, but are actual usage figures. This seems to indicate that employees will respond favorably to a non-intrusive reminder. As there was not a single instance of an employee complaining about the short reminder popping up on their screen it seems as if the employees did not mind the reminder. However, future research is needed to make this clearer. It is not clear how long this effect lasts however, and the next part of this research study will try to determine how the duration of effectiveness.

There was some concern over how to rate the various websites, as there is not a standard metric to go by here. The web traffic to the ‘mixed’ sites went down by 3% after the treatment, so including mixed with wasted would have made the numbers better. However it was decided to take a conservative approach to this and put that traffic in a separate category. However, this brings up the need for some type of metric in this area so that future research results can be more consistent.

It was interesting to note that although small by comparison, the traffic to the internet radio web sites did not change after the treatment. This may be because the employees do not see this as an abuse of the company equipment, or it may be deemed as not a waste of time by the employees. This would seem to support the research of Van Slyke and Belanger, Roy and Oravec [23], [1], [18], [15]. This was one reason we gave internet radio a separate category, and did not include it in the ‘waste’ category.
While this research study did show a positive short term effect on mitigating employee internet abuse, further research is required to determine the long range effects of this type of treatment as well as add instances to lessen concerns of bias.

5.0 Conclusion and limitations

Non-intrusive reinforcement may offer one method of mitigating employee internet abuse in the workplace. The lost man hours can be a large expense for the corporation, while the time invested in the treatment that was used here is minimal.

One limitation of this study was the lack of an accepted standard or methodology for determining which sites are definitely work related and which are not. Perhaps the biggest confound in this area are the social networking sites. To reduce the effects of this confound for our study, we conservatively did not include these sites in the ‘waste’ category, but further research will help with this problem.

6.0 References


