https://doi.org/10.48009/2_iis_2007_214-219

EMPLOYEE INTERNET ABUSE: POLICY VERSUS REALITY

Jeffrey J. Johnson, Utah State University, Jeffrey.Johnson@business.usu.edu
Zsolt Ugray, Utah State University, Zsolt.Ugray@usu.edu

ABSTRACT

This study addresses the question of whether Management and Technical measures effectively prevent or reduce employee Internet Abuse. Recent literature suggests that there is concern among practitioners and academics regarding the potential for diminished productivity, wasting of time and other resources, and even legal liability due to personal Internet use on company time. Recommendations to counter these problems usually include technical measures (firewall policy) and management measures (Acceptable Internet Use Policy or AIUP).

Most studies to date have relied on subject self-reporting to assess these potential problems. In our study we examine the actual Internet log file of an international company. We compare the declarations in the company's AIUP with the actual Internet use patterns in the log file. We also assess the effectiveness of the company's firewall policy by noting the types of web sites that are blocked, compared to the types that are not blocked.

This study sheds light on the gap between currently recommended measures and the reality of personal Internet use in the workplace. Our findings have implications regarding effective policy formulation and enforcement of interest to both managers and educators.

Keywords: Internet Abuse, Ethics, Acceptable Internet Use Policy

INTRODUCTION

The use of the Internet and the applications running on it, such as the World Wide Web and electronic mail, is an essential part of conducting business for many enterprises. It is not hard to argue that for many corporations a very large portion of regular activities involve not only the use of stand-alone computers but also the use of networked computers, most of the time all of them connected to the Internet. The line between appropriate and inappropriate use of the Internet is not trivial. Companies apply a wide variety of standards that define what is acceptable and what is not acceptable use of the Internet. While there is general consensus on the potential risks of conducting business online, companies implement very different policies and technologies to ensure that their employees adhere to these standards.

This paper presents a case study of the reality at a medium size business with multiple locations around the world. We study the employees' general patterns of Internet use at work and contrast it to the policy of the company.

Internet Abuse

The use and abuse of the Internet by employees has been much studied, discussed, and researched recently. The topic is considered so important that the whole January 2002 issue of the Communications of the ACM was dedicated to it. There may be consensus on the idea that personal Internet use on company time occurs, but the extent and effect thereof appear to be mostly conjecture.

Belanger and Van Slyke [2] point out that sometimes activities that are not work-related are encouraged in order to facilitate the learning of a new technology (email, in their case.) Although it may seem as an improper use of technology, the effect on increased efficacy can lead to the acceptance of the technology and increased productivity on the long term. Other authors suggest that "play" time is an essential ingredient in employee morale and therefore, indirectly, in productivity. For example, Oravec [6] asserted, "Constructive use of online recreation and play can enhance workplaces and perhaps ultimately make them more productive."

On the other hand, many authors have warned against the potential risks of employee Internet access. Lost productivity, wasting of time and other resources, legal liability, and addiction are examples of the ills associated with unrestricted employee Internet use. For example, see Greenfield and Davis' study [2]. Excessive use of the Internet can be a result of addiction. Young [6] defined criteria to determine Internet addiction as a clinical phenomenon. She also explored the effects of addiction and listed employee internet abuse as one of them.

Thus, use and abuse of the Internet by employees is a complex topic, with no clear answers or absolutes. The purpose of this study is to explore the reality of employee Internet use and abuse in a real-world setting, and to consider the effectiveness of management policy statements and technical enforcement measures.

RESEARCH METHODOLOGY

In most companies, access to the Internet is provided through a gateway computer. This is a natural location for a firewall and logging software that monitors and logs all in- and out-bound Internet communication. The log file can be a very rich source of data reflecting employees' online behavior [5]. IP addresses of senders and receivers for all Internet requests are recorded along with the common web addresses, known as Uniform Resource Locators (URLs), and the exact time of the requests. This information along with several other variables from the log file makes it possible to categorize the sites that each employee, identified by the IP address of a computer, visits from work. Added analysis can also shed light on the amount time an employee spends on each site along with the category of the content of those sites or the amount of bandwidth consumed by those visits.

For this study we analyzed the log file of a medium-sized international company with several locations in North America, Europe, Asia, and the Pacific. The company is in the business of manufacturing bio-medical and scientific instruments. We identified over 500 separate IP addresses within the company from the log file. We can safely assume that each address corresponds to a unique employee. Neither the company can be assumed to be representative of all companies, nor can its employees be assumed to represent all employees. However, the fairly large number of unique employees and the geographic diversity of the company's locations lends a certain level of confidence in the generalizability of our findings.

The company granted us access to the log file subject to a non-disclosure agreement. Individual employees' privacy was protected by hiding their identity and making it impossible to trace back the IP addresses to the actual computers. A list provided information about the geographical (i.e. country) location of the IP addresses.

Categorizing software was used to determine the type of web sites visited by each employee. While many web sites are immediately recognizable by their URL, (for example, www.ESPN.com for sports, www.CNN.com for news) the multitude of web sites "out there" and the volume of data in the file make automated help a necessity for log file analysis. The categorizing software assigned up to three category codes to each URL.

In a company, determination of which categories are to be considered appropriate or inappropriate would most likely be made by management, based on the activities of its employees, the industry in which they do business, and other factors. In this study, the researchers made assumptions about which categories should be considered appropriate. The categories we assumed to be considered as inappropriate are listed in Table 1. All possible categories, to which the software might assign a given web site, are listed in Appendix B.

RESULTS

The log file contained representations of all Internet transactions (CONNECT, GET, and POST calls, in addition to DENIED transactions) that occurred in the company over a four-week period. The file contained over six million lines, each containing the IP address of the user (company employee), the web site name (URL), and other information. Each line represents one transaction.

The Acceptable Internet Use Policy at the company is extremely simple. It consists of four statements, which we considered individually. The first establishes the fact that Internet and company-owned computer use is to be governed by the AIUP and other documents the company may produce from time to time. As this was the only document provided to us, we assume it was the only document addressing employee Internet use at the time of our study. The second statement is an unqualified prohibition of the use of "Internet and company computers for personal use". Taken at face value, this statement seems to leave no room for equivocation: no personal use is to be allowed. The third statement is nearly identical to the second, prohibiting personal commercial use, again with no room for doubt as to its meaning or intent. The final statement asserts the right of the company to monitor employee usage of computers, voice mail, e-mail, and the Internet. See Appendix A.

Previous consideration of the data revealed that employees do not comply with the apparent intent of the policy statement [3]. Of course management policy is nothing unless it does more than simply exist; it must be enforced. For Internet use, the

obvious enforcement solution is to employ a firewall, a software program that can block or deny incoming Internet traffic that is deemed to be undesirable. The firewall keeps a continuous record (log) of all Internet transactions. Our data consisted of a four-week extract of the firewall log. Of the six million Internet calls in our data set, 162,854 were DENIED by the firewall. If the management policy of no personal Internet use is to be taken literally, then the firewall appears to have failed to enforce the policy. The following paragraphs explain why.

Recognizing Inappropriate Internet Use

Identifying Internet abuse via log files is not always easy, because there may be legitimate reasons for a visit to many web sites that at first appear inappropriate. For example, the categorizing software we used identified over 200 thousand calls to sites in the "entertainment" category. Certainly "entertainment" could be considered an inappropriate use of company time and resources. On the other hand, many of the 200 thousand calls may represent employees using Interent radio to play harmless background music at their desks. Three more examples illustrate: first, if the log shows that a certain user visited an online auction site, does that mean the user was abusing her Internet privileges? Perhaps she was doing some personal shopping on company time. On the other hand, maybe this employee works in the purchasing department, and a significant part of her job is to find good prices on the Internet for the company supplies she is responsible to acquire. Second, suppose the log indicates an employee has been visiting a stock trading site at frequent, regular intervals. All day everyday, according to the log, this employee is presumably checking stock prices, every 60 seconds or so. Is he neglecting his duties while he hyperactively trades stocks all day? More likely, he has installed an automatic "ticker" which continually displays information across the bottom of his computer screen. While he may occasionally glance down to see how a particular stock is doing, he probably remains productive, and should not be considered an abuser. Finally, even something that may seem obvious, such as a pornography web site, if it shows up as a single, one-time entry may not necessarily signal abuse. Rather, it may be either a mistake (someone misspelled a web address) or an unwelcome pop-up window. In either case the employee immediately closed the window and did not return to the offensive site.

Still, "personal use is prohibited" could mean all of these examples should arouse suspicion. In our data, we counted the number of GET calls (that were not DENIED) in several categories we assumed would be deemed inappropriate for most businesses as shown in Table 1:

Table 1: Web Sites in "Inappropriate" Categories

Code	Category	Frequency of GET calls	Number of Users
cs	Criminal skills	474	20
et	Entertainment	293,561	351
fk	For Kids	4,130	51
gb	Gambling	11,312	49
gm	Games	52,019	147
hm	Humor	41,718	95
mm	Dating/Social	43,899	139
nd	Nudity	19,107	49
pa	Provocative Attire	43,824	108
sm	Sexual Material	31,329	62
sx	Pornography	70,379	89
pp	Personal Pages	58,714	250
pr	Profanity	14,421	45
sc	School Cheating	78	2
sp	Sports	171,753	198
su	Spam URLs	5,211	133
tb	Tobacco	556	9
tg	Gruesome Content	19,472	58
vi	Violence	1,317	20

While there is some overlap among the different categories (one web site may fall into more than one category) the number of users and the frequency of calls that were not DENIED, indicate that the firewall does not adequately enforce the "no personal use" policy. It is also important to note that one visit to a web page may require several GET calls. For example, the two employees who made 78 GET calls to sites categorized as "sc" or "school cheating" most likely did not visit 78 different web sites. Rather, depending on the composition of the sites, they probably visited no more than two or three sites each.

DISCUSSION

Access to the Internet provides employees with resources at a level that might previously have been considered unimaginable. The potential for acquiring information on a seemingly infinite number of topics, reaching target markets and being reached by sought-after providers, finding resources of all kinds, etc., explains why the Internet is generally considered a

boon to modern business. Unfortunately, the potential for productivity loss, wasted time and other resources, addictive behavior, and even illegal activities also is associated with business use of the Internet. Attempting to capitalize on the good while forestalling the bad, companies create policies for Internet use on two levels: management and technical. The management level is observable in the Acceptable Internet Use Policy or AIUP. The AIUP defines the rules for employee use of the Internet. The technical level is manifest in the firewall software used by the company. However, if other companies follow a pattern similar to the one in this study, there is a disconnect between the requirements of policy and actual Internet use. We can speculate reasons for the disconnect.

First, the firewall policy may bear no resemblance to the AIUP. That is, it is possible for rules to be specified in the software that are not based on management's dictates, but on a programmer's whims. The underlying reason for such disparity might conceivably be a lack of technical understanding on management's part. Perhaps the minutiae of network management, including firewall installation and setup, are left to the technical staff with no particular accountability for specific details. Therefore setting specific rules for blocking web sites is delegated by default to the network administrator or to the vendor.

Another possible explanation is that the AIUP is not adequately communicated. Many companies require that their employees sign a document affirming that they have read and understand the AIUP. But if the AIUP is not continually displayed or emphasized in some other way, it easily may be forgotten.

Additionally, the firewall policy may not be sufficiently broad to cover or block all possible violations of the AIUP. One occurrence found in our data illustrates this possibility: A specific user apparently was DENIED on several attempts to access web sites in the "sx" or "pornography" category. Undaunted, the user visited similar sites that were written in Spanish. Clearly, the firewall was blocking key words in the English language, but allowing the very same words in other languages to go through. This problem seems to be particularly pertinent in the environment of an international company such as the one we studied. Of course, the difficulty of listing all the potential key words in an ever-increasing list of languages, and thus the near impossibility of establishing perfect policy enforcement via a firewall here becomes apparent.

CONCLUSION

Because this study is a one-shot case study, our findings are not generalizable to every company. On the other hand there are lessons that may be learned from this company's experience both for practice where applicable, and for academics. First, a strong statement of policy combined with weak enforcement does little to protect a company from the potential ills of unfettered employee Internet use. Wasted time, bandwidth, and brainpower are only the beginning of problems potentially faced by a company that will not or can not enforce sound Internet use policy. There is clearly a dilemma here. While some academics have advocated loose policies, the line between appropriate and inappropriate personal Internet use is poorly defined if it is defined at all. If the goal is simply to write a policy statement then perhaps the easiest approach is to prohibit all personal use. However, this policy may actually be impossible to enforce completely, thus putting the company into a position of choosing when to enforce and when not to enforce – a legally difficult position. On the other hand, while a looser policy may be easier to enforce, by definition it allows for some personal use, including the ills which potentially accompany personal use.

Neither decision seems to be ideal. In an imperfect world, perhaps the best a company can do is to create a strong policy, exert reasonable effort to enforce it, and hope that catastrophe will not strike. Our conclusion is that while this path seems to be the best available option, it is not sufficient to protect against the ills associated with employee personal Internet use.

Further study of the phenomena associated with employee Internet use is warranted. The stakes are potentially high, including poor performance or even job loss for individuals, and resultant effects for companies ranging from non-competitiveness to legal liability. Understanding all of the reasons, outcomes, successes, and failures in this area is essential for preventing undesirable developments in a wide array of organizations and enterprises.

REFERENCES

1. Belanger, F. @ Van Slyke, C. (2002). Abuse or Learning? Communications of the ACM, 45(1), 64-65.

2. D. N. Greenfield and R. A Davis, "Lost in Cyberspace: The Web @ Work", CyberPsychology & Behavior, Vol. 5, No. 4, Mary Ann Leibert, Inc., August 2002.

3. J. Johnson and K. Chalmers, "Identifying Employee Internet Abuse" Proceedings of the Fortieth Annual Hawaii International Conference on Systems Sciences (HICSS), Wailkoloa Hawaii, January 3-6 2007.

4. J. Oravec, "Constructive Approaches to Internet Recreation in the Workplace. Communications of the ACM 45, 1 January 2002.

5. Schweitzer, D. (2005). Don't Ignore Lowly Log Analysis. Computerworld, January 24.

6. Young, K. S. (2004). Internet Addiction: A New Clinical Phenomenon and Its Consequences. American Behavioral Scientist, 48 (4), 402-415.

APPENDIX A

This "official" policy of the company is somewhat softened by an e-mail message from management to the effect that supervisors may approve limited personal Internet use.

Voice mail and E-mail use are addressed separately in similarly strong language.

"Company Code of Conduct:

The use of the internet, company computers and other company property is subject to this code and to such other policies and procedures as the company may implement from time to time. The use of the internet and company computers for personal use is prohibited. The use of the internet and company computers for personal commercial use is prohibited. The company may at any time for any reason monitor the use of company property, including computers, voice-mail, e-mail, or access to and use of the internet."

APPENDIX B

The following table lists all the categories to which the software might identify a given web page. The vendor continuously updates a database to keep the categories current.

ac	Art/Culture/Heritage
al	Alcohol
an	Anonymizers
au	Anonymizing Utilities
bu	Business
ch	Chat
ci	Computing/Internet
cm	Consumer Information
cs	Criminal Skills
cv	Game/Cartoon Violence
dr	Drugs
eb	Auction
ed	Education/Reference
et	Entertainment/Recreation/Hobbies
ex	Extreme
fi	Finance
fk	For Kids
gb	Gambling
gm	Games
gr	Gambling Related
gv	Government/Military
hi	History
hk	Hacking
hl	Health
hm	Humor
hs	Hate Speech
im	Instant Messaging
in	Stock Trading
ir	Internet Radio/TV
js	Job Search
mb	Forum/Bulletin Boards
mg	Messaging
mm	Dating/Social
mo	Mobile Phone
mp	Media Downloads
mr	Moderated (exception)
ms	Malicious Sites
na	Usenet News
nd	Nudity
np	Non-Profit Organizations/Advocacy Groups
ns	Personal Network Storage
nw	General News
os	Shopping/Merchandizing
pa	Provocative Attire
ph	Phishing
pn	P2P/File Sharing
po	Politics/Opinion
pp	Personal Pages
pr	Profanity
ps	Portal Sites
ra	Remote Access
rl	Religion and Ideology
rs	Resource Sharing
sc	School Cheating Information
se	Search Engines
sm	Sexual Materials
sp	Sports
st	Streaming Media
su	Spam Email URLs
sw	Shareware/Freeware
sx	Pornography
sy	Spyware
tb	Tobacco
tf	Technical/Business Forums
tg	Gruesome Content
to	Text/Spoken Only
tr	Travel
u0	User Defined Category 0
u1	User Defined Category 1
u2	User Defined Category 2
u3	User Defined Category 3
u4	User Defined Category 4
u5	User Defined Category 5
u6	User Defined Category 6
u7	User Defined Category 7
u8	User Defined Category 8
u9	User Defined Category 9
UK	Unknown
vi	Violence
vs	Visual Search Engine
wa	Web Ads
we	Weapons
wm	Web Mail
wp	Web Phone