THE EFFECTS OF AN ACCEPTABLE INTERNET USE POLICY ON EMPLOYEE PERSONAL INTERNET USE

Jose Limas, Jon M. Hunstman School of Business, Utah State University, 3515 Old Main Hill, Logan, UT 84322, 435-730-1841, jose.limas@usu.edu
Jeffrey J. Johnson, Jon M. Hunstman School of Business, Utah State University, 3515 Old Main Hill, Logan, UT 84322, 435-797-2350, Jeffrey.Johnson@usu.edu

ABSTRACT

This study attempts to assess the effectiveness of a new Acceptable Internet Use Policy (AIUP) in a small company. Through management interviews and log file analysis the goals and results of the policy change were assessed. A model based on the Theory of Reasoned Action (TRA) is employed. By implementing measures beyond publication of a document, managers were successful in curtailing employees' undesirable Internet use on the company's network.

INTRODUCTION

Internet use in the workplace has become widespread because employers view it as something positive. However, some research attention has been directed at the phenomenon of employee Internet abuse, or in less provocative terms, personal web use. Many of the papers published in the last decade extol Acceptable Internet Use Policies (AIUPs) as a necessity for effective management of an employee activity that has at least the potential for detrimental effects on productivity, bandwidth use, legal liability, and more. Conversely, some authors posit that personal web use is not deleterious and may have some positive effects on employee morale or other aspect. In essence, employee Internet use can produce positive and negative results. Managing for maximization of the positives and minimization of the negatives is the obvious challenge for today's Internet-enabled organizations.
Implementation and enforcement of an AIUP are intended to address the challenge. But questions arise about the effectiveness of AIUPs. This study examines one company's attempt to meet the challenge of managing employee Internet use by creating and implementing a new AIUP.

RELATED LITERATURE

Employee Internet use and abuse has become a popular topic for academic research in recent years. Articles in trade magazines and newspapers have also appeared, mostly warning against the dangers of unfettered employee web surfing. Other authors counter with examples of positive outcomes and beneficial effects of employee Internet use. A few examples of published articles emphasizing both sides of the managing-employee-Internet-use challenge follow:
Anandarajan & Simms [1] investigated respondents' attitudes about "Personal Web Use," and found that while potential negatives were acknowledged by employees who participated in their survey, positive effects were also asserted. Increased skills and knowledge, productivity gain, balancing work and life, and reducing stress were cited as potential constructive outcomes. Oravec [9] similarly asserted that employees may actually increase their own value to their employer by exploring and learning on the Internet.

Lim [7] found that employees may engage in "neutralizing" or justifying their web surfing with a sense of organizational justice. Long hours, lack of appreciation, and taking work home are examples of reasons employees may feel justified (the company owes it to them) in surfing on company time.
Sipior & Ward [11] noted that organizations' efforts to curtail employee Internet abuse, especially if those efforts include Internet and Email monitoring, can have the unintended consequence of infringing on legitimate employee privacy expectations. This only complicates the multifaceted challenge of managing Internet use effectively. The same authors listed copyright infringement, defamation and libel, discrimination, harassment, hostile work environment, obscenity, pornography, violations of securities laws, violations of trademark and trade secret laws, and loss of employee productivity and Internet resource use as potential threats from within an organization
Thatcher, Wretschko, Fridjhon [12] found a connection between "problematic Internet use, "flow" (a state of mind characterized by loss of a sense of time, among other things) and procrastination. They concluded Internet use entails such a broad array of diverse activities that it should be studied at a level of finer granularity. Employee Internet use can be interpreted correctly only if we know what kind of Internet activity is being conducted.
With similar intent, Anandarajan, Paravastu, and Simmers [2] divided study participants into three groups, based on their reported Internet-related behavior: Cyber-bureaucrat, cyber-humanist, and cyber-adventurer. By their reasoning, an organization's interests would be served best by multiple polices addressing different kinds of users, rather than a one-size-fits-all policy.
One obvious conclusion from the literature is that managing employee Internet use is a complex task, requiring at least some kind of balance to encourage positive work-related and productivity-enhancing Internet use while curtailing potential negative outcomes. Published AIUPs are widely recommended and applied (for example [3], [10]). However, as noted in other articles [5],[6], a few sentences on a piece of paper are not necessarily effective by themselves. Enforcement and coordination with technical policy (i.e. firewall policy) are also required. Tellingly, Mastrangelo, Everton, and Jolton [8], who distinguished between computer use that is counter-productive and that which is merely non-productive found certain conditions (younger employees, longer access at work, and faster connections at work than at home) seemed to contribute to non-productive use, while other conditions (newer Internet access and knowledge of other employees being warned about Internet misuse) seemed to contribute to counterproductive use. In their words, "the likelihood that an employee will engage in deviant computer use does not change depending on employee awareness of their computer use being monitored." [8 p. 739]
In summary,

- Employee Internet Use produces enough positive effects to justify access in many companies.
- Granting employee Internet access exposes organizations to potential negative consequences, some of which can be very serious
- AIUPs are recommended as management tools but under some circumstances employees may ignore or circumvent written policies.

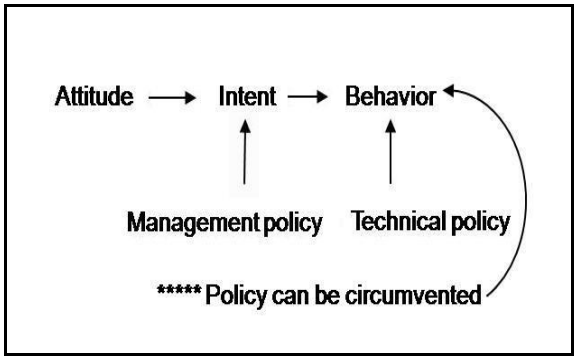
Therefore the question for this study is whether implementation of an AIUP can effectively reduce unwanted Internet use behavior.

CONCEPTUAL BACKGROUND

Explaining human behavior via Theory can be useful in understanding and managing employee behavior. Among many behavioral theories available, few have been as widely applied as the Fishbein's and Ajzen's [4] Theory of Reasoned Action. According to this theory, attitude is one determinant of intent to perform a certain behavior, and intent is a determinant of the actual behavior. Based on these

ideas, we propose the following model. We understand AIUPs to be an attempt by management to influence employees' intentions regarding their Internet use.

FIGURE 1. MODEL OF POLICY'S IMPACT ON BEHAVIOR



However, since existence of a written management policy (even if employees are well aware of it) may not be sufficient to influence behavior, firewall policy is also implemented to restrict employee Internet use behavior within acceptable boundaries (among other reasons).

We note that if the employee's attitude is not in conformance with management policy, the policy may be ignored (as described by Mastrangelo, Everton and Jolton [8]). If so, the firewall policy may still deter undesirable internet use. However, Johnson & Chalmers [5] noticed that deviance-motivated employees also can circumvent firewalls, in some cases even without extensive knowledge or understanding of the details of the technical policy. Thus, we adopt the model in figure 1.

METHOD

Most studies of employee Internet use and abuse to date have relied on self-reports/surveys of employees. Our intent in this study was to capture actual behavior and attempt to explain it vis-à-vis management's intentions as operationalized in their AIUP. The methods employed for this study included brief interviews of two managers at a company, and analysis of log file data before and after implementation of a new AIUP. Both authors attended and participated in the interviews. Notes were subsequently compared and correlated. Both managers later responded to follow-up and clarification questions.

Data from the company's Internet log file was provided in Microsoft Access Database format. Each line of the data included the Internet Protocol (IP) address of the employee, the web address of the site visited, and the date and time of the visit, along with other data. The total number of records, representing the company's Internet activity over a period of six months, exceeded one million. Simple numerical comparisons were made of log file characteristics from before and after implementation of a new AIUP.

RESULTS

The company is a small title company (roughly 100 employees) which processes home mortgage title searches. The purpose of the interviews was to gain understanding of the company's motivation for implementing a new AIUP, from the perspective of a manager in charge of IT security, and from one in charge of employee productivity.

Interviews

Two managers at the company were interviewed. The first (manager A) was the Vice President of Information Technology and the local branch manager. The other manager (manager B) was director of Information Technology for the company. Manager A's main concern was employee productivity. He spoke of wasted time and work delays due to inappropriate or non work-related Internet use.
Manager B said his main worry was the integrity and security of the company's information systems. He spoke of performance-degrading spyware, and other malware such as viruses etc. that can gain entry due to careless Internet activity.
Both managers were asked about AIUP implementation, employee education, and enforcement. Manager A desired productivity without creating an oppressive environment, believing that happy employees would be more productive, easier to retain, more pleasant to work with, than disgruntled employees would be. Thus his desire to protect productivity was tempered by his desire for a congenial working environment. Therefore strict enforcement had never actually been implemented. Rather, employees were shown the old AIUP document when hired, and reminded annually at their performance review and during other company training meetings about the policy and its penalties. Using an open (no walls) office layout without private work areas, enforcement was indirectly achieved by peer pressure and a lack of private opportunity for Internet abuse. The net effect of Manager A's philosophy was incomplete enforcement of the "no personal Internet use" policy.
Manager B was concerned with security and privacy regarding the data on customers' mortgage applications. The open office environment thwarted his efforts to protect customer data. Online E-mail accounts were particularly offensive to him because of their potential to introduce undesirable security risks to the company's network, data, and systems. His proposed solution was to install monitoring software on each workstation, and to aggressively enforce the AIUP penalties, including monetary fines (increasing with each violation) and ultimately, termination.
Tension was apparent due to the differing philosophical stances of the two managers. Their problem was to develop a solution which would ensure data security and system integrity without encumbering the pleasant work culture. They needed a workable, enforceable policy that would:

- Protect the company's interests (productivity, data integrity, etc.)
- Preserve employee morale, avoiding the counter-measures of "neutralizing" (rationalizing) employees

Their solution was to create and implement a new AIUP. But the policy entailed more than a framed document on the wall. While it did include written rules and penalties for violation, it also involved restructuring the company's intranet, and a renewed commitment from management to enforce the written policy. The main features of the new policy included:

- An Internet Café consisting of a few unmonitored, internet-capable computers, physically separate from employees' workstations, and on a separate sub-net of the company network. These computers are for non work-related, personal use only. They are accessible to employees before and after regular work hours, and during lunch and other breaks. They were located in a public area, where social pressure indirectly enforced decency and other standards.
- Online E-mail accounts are allowed on the Internet Café machines.
- A graduated schedule of fines established to discourage personal Internet use on regular workstations. Enforcement was made possible via log file analysis.
- Personal Internet use on regular workstations is disallowed.

This policy, the managers hoped, would encourage employees to be both productive and compliant. Personal web use would not be oppressively denied, but productivity and security would be preserved. The effectiveness of the policy, in terms of changes in employee Internet use behavior is described

below. Changes in employee productivity are not reported here because we were not given access to productivity data.

Log file analysis

The sample data used for our study was collected over a six month period. The software used to analyze the website usage was WaveCrest Cyfin Reporter, which categorizes the websites into 69 categories and three classes. We broke our data down into two groups: Group 1 included all log file entries for the three months prior to implementation of the new policy. Group 2 included entries for the three months after implementation of the new policy. For the purpose of this study, we define a website "hit" as anything that generates a line in the log file. The data in Group 1 contained 30,201 website hits during the three months immediately prior to the new AIUP and internet cafés being introduced. Group 2 contained 2,578 website hits during the three months after the new AIUP and internet cafés were introduced.

The websites were then categorized into one of the 69 categories provided by WaveCrest Cyfin Reporter and then grouped into three distinct classes; acceptable, unacceptable, and neutral. For our study we only looked at the acceptable and unacceptable classes as indicated by the WaveCrest Cyfin Reporter. A list of categories with brief descriptions and their classes appears in Appendix A.

The data from Group 1 had 11,232 unacceptable website hits constituting 37% of total website hits during the three month timeframe. Group 2 had 212 unacceptable website hits constituting 8% of total website hits during the three month timeframe.

Total website visits dropped from 30,201 to 2,578 while the total number of unacceptable website visits dropped from 11,232 to 212. Five categories of sites visited in the top ten of Group 1 dropped out of the top ten in Group 2's results. The top two categories visited for Group 1 dropped entirely off the list of categories visited in Group 2.

Forty-four of the 69 categories categories provided by WaveCrest Cyfin Reporter were represented in the Group 1 data. Group 2 had websites that fell into only 21 of the 69 categories.

For Group 1, the top ten categories, as determined by total number of hits in each, included only two that were classified as "Acceptable". Six of the top ten categories for Group 2 were in the "Acceptable" class.

Five of the categories in Group 1's top ten had were in the "Unacceptable" class while Group 2 had only two of the top ten categories that were in the "Unacceptable" class. The top ten categories for both groups had two categories in the "Neutral" class. The top ten categories prior to the implementation of the new AIUP were as shown in Table 1:

TABLE 1. TOP 10 CATEGORIES PRIOR TO THE IMPLEMENTATION OF NEW AIUP

Site Category	Total Hits	Class
Travel	2527	Unacceptable
Shopping	2422	Unacceptable
Health and Medicine	1685	Acceptable
Government	1477	Neutral
Vehicle	1229	Unacceptable
Banners-Ads	1088	Neutral
Food & Drink	1037	Unacceptable
Education	658	Acceptable
Financial	616	Unacceptable
News and Media	520	Acceptable

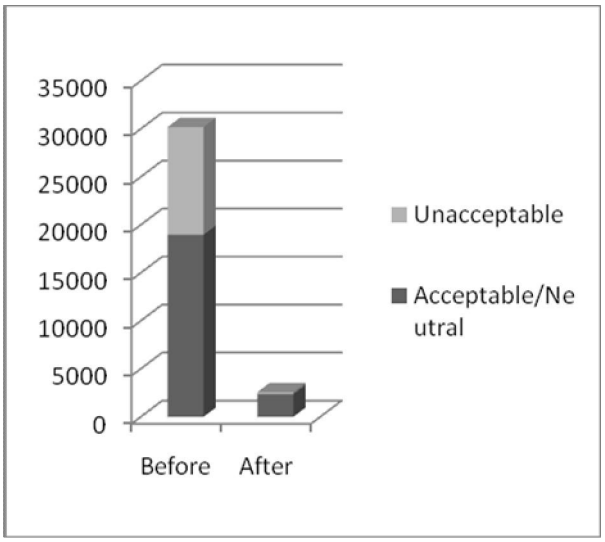
TABLE 2 TOP 10 CATEGORIES AFTER THE IMPLEMENTATION OF NEW AIUP

Site Category	Total Hits	Class
Government	321	Neutral
Regional Information	238	Acceptable
Hardware Software	206	Acceptable
Legal	157	Acceptable
Banners-Ads	156	Neutral
Health and Medicine	65	Acceptable
Food and Drink	53	Unacceptable
News and Media	53	Acceptable
Reference	51	Acceptable
Vehicles	51	Unacceptable

Source: Title Company Weblog Analysis via WaveCrest Cyfin Reporter

After implementation of the new policy, overall Internet activity decreased from 30,201 log file lines (hits) to 2,578. Of all traffic before the new policy implementation 11,232 or 37% fell into the "Unacceptable" class. After implementation of the new policy 212 or 8% were classified as unacceptable. See Table 2 and Figure 2.

FIGURE 2. BEFORE AND AFTER IMPLEMENTATION OF AIUP



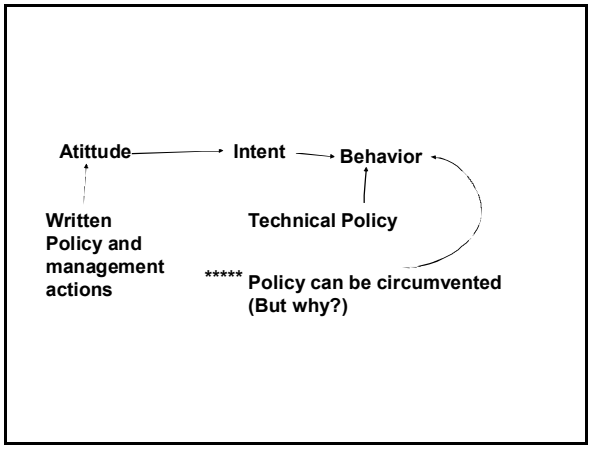
DISCUSSION

The dramatic reduction in Internet traffic after implementation of the new policy is partly due the fact that traffic from the Internet Café machines is not included in this log. Still, the reduction is impressive for the company's "work" network. If traffic has simply been re-routed to another network, the company's goals are still accomplished because the "work" network is now relatively free from threatening activity. Additionally, the reduction in percentage of "Unacceptable" traffic indicates that

the policy is effective in curtailing Internet use behavior that constitutes a threat to the company's data and information system resources.

Based loosely on the Theory of Reasoned Action, our model included the real possibility that enterprising employees can find ways to circumvent written policy and can even defeat firewall policies. Recognizing this reality, the managers in this company sought to meet their own goals (security and productivity) without giving employees a reason or implicit challenge to circumvent management's efforts. They succeeded by expanding the scope of their efforts beyond a simple document and firewall. The new policy did include a written document, and firewall rules were executed, but additional measures including installation of "Internet café" stations were also taken. Such imagination and creativity on the part of managers, with consideration for factors such as the company culture, physical layout of the office, and arrangement of network topologies, are certainly apropos. Therefore, we would expand the definition of "management policy" to include much more than a simple written document, no matter how often or how forcefully employees' attention might be drawn to it. Perhaps our model can be modified to emphasize that policy should be more than just a document. A more comprehensive perspective of policy, including considerations such as those listed above, might go beyond employees intentions and actually affect employee attitudes. Thus, if, as in this case, policy includes consideration of likely employee behavior, and policy is more than a document, then employees might not have an inclination to circumvent it.

FIGURE 3. ADJUSTED MODEL



Given the conflicting desires of management to provide uncompromising system security while permitting enough employee Internet access to reap such benefits as morale and learning, the new policy seems to be a success. However, a one-shot case study is insufficient to provide empirical or generalizable proof. Rather this study provides another point of consideration in the ongoing conversation about how to manage the complex and unwieldy challenge of personal Internet/Web use at work.

APPENDIX A

(U)= Unacceptable (A)=Acceptable (N)=Neutral	***Category Description***
Agriculture (A)	*Farming, Ranching, Forestry, related products, activities, and information.*
Auction/Classified (U)	*Auctions, Classified Ads, Personal Sales, related activities and information.*
Banners/Ads (N)	*Electronic Banner Ads, related activities.*
Business Services (A)	*Printing and Publishing, Office Supplies, Consulting, Accounting Services, related activities.*
Chat (U)	*Web-Based Chat, related activities.*
Construction (N)	*Architect Services, Construction Contractors, Construction Methods, related activities and topics.*
Cults (U)	*Cults, Paganism, Satanism, Alternative Religions, related activities and information.*
Download (U)	*Download "Hits" tagged onto an Internet visit, such as a downloaded file. Not an actual category.*
Download Sites (U)	*Freeware, Shareware, related activities.*
Drugs (U)	*Illegal Drugs, Formulation and Sale, Drug Paraphernalia, Recreational Drugs, related activities.*
Education (A)	*K-12, Colleges and Universities, Training, related activities and information.*
Entertainment (U)	*Movies, Television, Theater, Theme Parks, Fan Clubs and Sites, Recreation, related activities.*
Environment (A)	*Air and Water Quality, Conservation, Waste Management, Ecology, Animal Protection, related activities.*
Fantasy Leagues (U)	*Virtual Sports, sometimes offering rewards to participants.*
Financial (U)	*Investment Services, Banking, Bankruptcy, Loans, related activities and information.*
Food and Drink (U)	*Restaurants, Cafes, Diners, Bars, Pubs, Recipes, Cooking Instructions, Beverages, related information.*
Gambling (U)	*Gaming, Virtual Casinos, Physical Casinos, Offshore Gambling, Lottery, Sports Advisory Services, related info.*
Games (U)	*Download Games Sites, Online Games, Computer Games, Video Games, related tips and information.*
General Blogging (N)	*Sites that contain people's online 'diaries' which may contain wide range of images and text.*
Government (N)	*Federal Government, State and Local Government, Government Functions and Services, related information.*
Hacking (U)	*Computer Crime, Promotion or advice about hacking passwords, creating viruses, related information.*
Hardware and Software (A)	*Computer Hardware and Software, Computer-Related Publications, Internet Information (non-ISP).*
Hate and Crime (U)	*Hate Speech, Racism and Racial Bigotry, Terrorist Activities, Criminal Activities, related information.*
Health and Medicine (A)	*Hospitals and Clinics, Physicians, Pharmaceuticals, Health Foods, Diets, related information.*
IP Address (N)	*Numerical IP Addresses, not named web sites.*
Insurance (A)	*Life Insurance, Health Insurance, Automobile Insurance, Homeowner's Insurance, related information.*
Internet Services (A)	*Internet Service Providers (ISPs), Web Site Hosting, Web Site Design Services, related information.*

Job Search (U)	*Employment, Job Placement, Resume Assistance, Recruiting (non-military), related activities and info.*
Legal (A)	*Law Enforcement, Courts, Lawyers and Litigation, Civil Rights, related activities and information.*
Manufacturing (A)	*Traditional Manufacturing, Mining, related activities and information.*
Marketing (A)	*Marketing, Advertising, related services, activities and information.*
Mutlimedia (U)	*Image "Hits" tagged onto an Internet visit, such as a .jpeg or .gif. Not an actual category.*
Military (N)	*Military Web Sites, Military Bases, general military information, related activities.*
Music Radio/Downloads (U)	*Streaming radio, music downloads such as .mp3 files.*
News and Media (A)	*TV Networks and Stations, Radio Stations, News Organizations, Online Newspapers, related information.*
Non-Profit Organizations (N)	*Charitable Organizations, Veterans' Organizations, Emergency Help Organizations, related info.*
Other (A)	*Sites not previously categorized by Wavecrest Computing.*
Personals and Dating (U)	*Dating Services, Matchmaking, Mail Order Brides, Personal Ads, Singles Groups, related information.*
Phishing/Fraud (U)	*Fraudulent Internet Operations, fake emails that attempt to obtain personal and financial information.*
Politics (U)	*Political Advocacy, Political Party Organizations, related activities and information.*
Pornography (U)	*Explicit Sex Images, Adult Video Sales, Sex Toys, Prostitution, Nudity, Prurient Sex Information*
Public Proxy (U)	*Anonymous Web Surfing, Web Activity Disguises, Remote Public Proxy, related activities and information.*
Real Estate (U)	*Housing, Home Ownership, Property Management, Real Estate Sales, Rentals, Home Services, related information.*
Reference (A)	*Dictionaries, Encyclopedias, Language Translation, Writing Guides, Maps, Libraries, related information.*
Regional Information (A)	*Localities, Local Events, Local TV and Radio*
Religion (U)	*Religious Advocacy, Houses of Worship, related activities and information.*
SSL (A)	*Secure Socket Layer "Hits". A type of secure connection such as "https" tagged onto a visit. Not an actual category.*
Science (A)	*Scientific Research, Scientific information and services*
Search Engines (A)	*Web Search Services, Search Directories, Search Portals*
Shipping (A)	*Material Shipping Services, Packing and Shipping Services, Mailing Services*
Shopping (U)	*Physical and Online Retail Activities and Stores, Shopping Aids, Shopping Information*
Social Networking (U)	*Social sites containing personal profiles with wide range of images and text for purposes of social interaction.*
Society and Culture (U)	*Pop Culture, Museums and Galleries, Society, Arts, Lifestyles, Hobbies, Operas/Plays, related info.*
Sports (U)	*Athletic Activities, Sports Scores and Information, Sports Teams, Hunting and Fishing, related activities.*
Spyware/Malicious (U)	*Sites and/or files that infiltrate computers and report Internet activity back to unknown sources.*
Stock Trading (U)	*Stock Quotes, Stock Tickers, Personal Stock Transactions.*
Streaming Media (N)	*Any live or archived streamed audio or video file, Personal Webcam Sites, related information.*
Tasteless (U)	*Offensive Information, Excessive Profanity.*
Telecommunications (A)	*Cable TV Services, Wireless Services and Products, Telecommunications Services and Products.*
Transportation (A)	*Commuter Transportation, Local Train Bus and Taxi Services, Local Transportation Schedules.*
Travel (U)	*Tourist Travel, Vacation Sites, Airlines, Hotels, Cruises, Rental Cars, Travel Agents, related information.*

Unsolicited or Push (U)	*Sites such as Infogate (formerly Pointcast), Microsoft Channels and Backweb.*
User News Groups (A)	*Internet User Groups, Software User Groups, related groups.*
Utility (N)	*Energy Exploration, Energy Processing and Refinement, Energy Distribution and Marketing, related information.*
Vehicles (U)	*Automobiles, Vehicle Design and Manufacturing, Boats, Motorcycles, Vehicle Clubs, related activities and info.*
Weather (A)	*Information on Weather and Meteorology.*
Web Email (U)	*Web e-mail, Online Email Services, related activities.*
Worthless (U)	*Sites that do not fall into any other category and seemingly serve no purpose.*
Youth (N)	*Sites aimed at children's interests.*

REFERENCES

[1] Anandarajan M. and Simmers, C.A. Developing Human Capital Through Personal Web Use in the Workplace: Mapping Employee Perceptions. *Communications of the Association for Information Systems* 2005 *15*, 776-791.

[2] Anandarajan, M., Paravastu, N. and Simmers, C.A. Perceptions of Personal Web Usage in the Workplace: A Q-Methodology approach. *CyberPsychology & Behavior* 2006 *9* (3), 325-335.

[3] Case, C.J. and Young, K.S. Employee Internet Use Policy: An Examination of Perceived Effectiveness. *Issues in Information Systems*, Still Water Oklahoma, 2002,. 82-88.

[4] Fishbein, M., and Azjen, I. Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research, Addison Wesley, Reading, Mass., 1975.

[5] Johnson , J.J. & Ugray, Z. Employee Internet Abuse: Policy versus Reality, *Issues in Information Systems*, Still Water Oklahoma, 2007.

[6] Johnson , J.J. & Chalmers, K. Identifying Employee Internet Abuse, *Proceeding of the 40th Hawaii International Conference on System Sciences*, 2007.

[7] Lim, V.K.G. The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice, *Journal of Organizational Behavior* 2002 *23*, 675-694.

[8] Mastrangelo, P.M. Everton, W. and Jolton, J.A. Personal Use of Work Computers: Distraction versus Destruction. *CyberPsychology & Behavior* 2006 *9* (6), 730-741.

[9] Oravec, J.A. Constructive Approaches to Internet Recreation in the Workplace. *Communications of the ACM* 2002 *45* (1) 60-65.

[10] Sian, K., Nah, F. & Teng, L. Acceptable Internet Use Policy. *Communications of the ACM*, 2002 *45* (1) 75-79.

[11] Sipior, J.C. & Ward, B.T. A Strategic Response to the Broad Spectrum of Internet Abuse. *Information Systems Management*, 2002, 71-79.

[12] Thatcher, A., Wretschko, G. & Fridjhon, P. Online flow experiences, problematic Internet use and Internet procrastination. *Computers in Human Behavior* 2008 *24*, 2236-2254.