A PRELIMINARY INVESTIGATION OF EMPLOYEE INTERNET MISUSE

Dr. Carl J. Case, St. Bonaventure University, ccase@sbu.edu
Dr. Kimberly S. Young, Center for On-Line Addiction, ksy@netaddiction.com

ABSTRACT

This paper examines the results of a preliminary investigation of employee Internet misuse. Prior research has been primarily in the form of industry-driven self-reported surveys regarding Internet monitoring. Such research suggests that Internet misuse is widespread. This case study examines Internet misuse utilizing a research framework. A survey instrument and interviews with business manufacturing firms are used to collect data. Results suggest that monitoring may not be as formal as previously indicated. In addition, enforcement may be generally in the form of informal reprimands.

Keywords: Internet misuse, Internet monitoring, Internet enforcement, case study

THE INTERNET RESOURCE

Organizations use the Information System (IS) function as a important mechanism in managing the Internet. IS professionals develop, implement, and maintain the telecommunications infrastructure. Moreover, these individuals may monitor, collect evidence, or control employee Internet use. And, the chief information officer may play a significant role in determining corporate Internet policy.

However, the number of users and amount of data available are still experiencing dramatic increases. According to a Websense, Inc. survey of human resource directors, approximately 70 percent of companies provide Internet access to more than half of their employees (11). In addition, Netsizer reports that there are more than 350 million Internet users worldwide (10). The number of Internet users was estimated to be 304 million in March 2000 and 171 million in March 1999 (12). Thus, in less than two years, the number of users worldwide has doubled. Moreover, Telcordia Technologies estimates that the number of Internet hosts has reached 100 million and grown by 45 in the past year (10). Cyveillance also released a study estimating that there are 2.1 billion unique Web pages, with a growth of 7 million pages per day (7).

Overall, the Internet is continuing its remarkable expansion both in terms of users and data. As a result, managing the corporate Internet resource may be more difficult and increasing in importance.

CORPORATE RESPONSE

To respond to the challenge, several products have been introduced. Software such as Insight, WinGuardian, and WinWhatWhere Investigator that are marketed for less than $100 allow organizations to inexpensively monitor Web use (8). Moreover, nearly 2000 companies nationwide

use a SpectorSoft monitoring system that captures a picture of an employee=s computer screen every one to 30 seconds for review by employers. Other similar software include Omniquad Desktop Surveillance and Softeyes (6).

By examining the media headlines, it is apparent that computer misuse is becoming problematic. Several predominant corporations have been affected. The New York Times fired 22 employees in Virginia for allegedly distributing potentially offensive electronic mail (2). Xerox terminated 40 workers for spending work time surfing pornographic and shopping sites on the Web. Dow Chemical Company fired 50 employees and suspended another 200 for up to four weeks without pay after an e-mail investigation uncovered hard-core pornography and violent subject matter (4). In June of 2000, Merck & Company disciplined and dismissed employees and contractors for inappropriate e-mail and Internet usage (5).

PRIOR RESEARCH

Prior research in the area of employee Internet misuse has generally been manifested in the form of industry-driven surveys. Studies have primarily examined Internet management from a monitoring perspective. Due to the non-academic basis of study, this research is fragmented with no apparent research framework in place to serve as a guide. The following surveys provide examples of prior research.

According to an American Management Association (AMA) survey, 74% of corporations use some form of monitoring software (8). The AMA estimates that 45% of companies with 1000 or more employees monitor electronic communications from workers (9). Moreover, the AMA indicates that approximately 38% of 2,100 major U.S. companies check their employee=s email and 54% monitor Internet connections (6). Of these organizations, 17% have fired employees, 26% have issued formal reprimands, and 20% have given informal warnings.

A survey of 670 companies by carrier site Vault.com also examined Internet monitoring (14). Results indicate that 41% of organizations restrict or monitor Internet use and four out of five employers surveyed stated they have caught employees surfing the Web for personal use during work hours. Just over one-third of respondents indicate that 10 to 30 minutes of Internet surfing per day for personal reasons is acceptable, while 25% state that 30 to 60 minutes does not pose a problem. Only 14.7% report that personal Internet use is not tolerated. Interestingly, 92% of employees and 82% of employers would support legislation requiring companies to notify workers if they plan to monitor Internet use in the workplace.

An *Information Week* research survey of 250 IT and business professionals found 62% of companies monitor its employees= website use (13). Approximately 60% monitor phone use, 54% monitor email, and less that 20% monitor productivity of home-office workers. Among companies larger than $1 billion, website and email monitoring jumps to 77% and 70%, respectively.

Another study was conducted by Websense, Inc., an Internet access management company (11). The survey of 224 human resource management (HRM) directors found that 83 percent of the companies

indicated they have Internet access policies (IAP). Even though IAPs exist, 64 percent of the companies have disciplined, and more than 30 percent have terminated, employees for inappropriate use of the Internet. Accessing pornography (42%), online chatting (13%), gaming (12%), sports (8%), investing (7%), and shopping at work (7%) were the leading causes for disciplinary action or termination. Approximately 50 percent of companies are not concerned about the problem and/or have done little to enforce the IAPs. 60 percent of the companies use self or managerial oversight and only 38 percent use filtering software.

In a September 1999 Vault.com survey of 1439 workers, 37 percent admit surfing constantly (1). 32 percent stated he/she surfed a few times a day while 21 percent surf a few times a week. As a result, Vault estimates $54 billion annually in lost productivity.

Telemate.Net Software, Inc., a provider of Internet usage management and eBusiness intelligence solutions, conducted a research study via the Internet and surveyed more than 700 companies from a diverse cross-section of industries (3). Survey respondents included executive, senior IT, and human resource managers. Findings indicate that 83 percent of surveyed companies were concerned with inappropriate employee usage of the Internet and the resulting legal liabilities and/or negative publicity. Over 70 percent indicated that surf abuse results in real costs to their companies in the way of additional network upgrades, lost productivity and slow network response.

Consequently, prior research has been limited to primarily industry-driven surveys. The research appears fragmented, with a few common themes, but without direction.

RESEARCH DESIGN

This study employs a multi-site case study research design to examine employee Internet management. Three northeastern U.S. manufacturing companies were utilized. An extensive Internet Management Assessment survey instrument was developed and administered to management responsible for the IS function. The instrument was utilized to collect company demographic data, assess management style, and examine employee Internet misuse and enforcement. In addition, management were interviewed on site by both researchers concurrently. Management included comptrollers, IS managers, and HRM management.

An Internet E-Management Framework was utilized to examine the organizations (Figure 1). Four constructs, identified as e-management, enforcement, job necessity, and e-behavior are hypothesized to impact productivity.

Enforcement and e-management are organization-level or macro constructs. E-management is the organization=s culture relating to their tendency of being proactive to Internet misuse. Possible proactive measures include screening, training, policy implementation, monitoring, or no measures. Enforcement can be stated as the organization=s tolerance or reaction to employee Internet misuse. Possible reactions include warnings, rehabilitation, dismissal, or no reaction, i.e., free use.

Job necessity and predominant e-behavior are employee-level or micro constructs. Job necessity relates to the percentage of time that the Internet is necessary to perform individual job functions relative to the individual=s total work time (daily hours necessary on Internet to perform duties / total hours per day productive). Predominant e-behavior includes dysfunctional behavior such as spamming, involvement in non-work related newsgroups, flaming, sending racist or sexual harassment electronic mail, chatroom participation, slacking (stocks, surfing, sports, newsgroups), cybersex, pornography, gambling, and security threats (hacking, copyright, transmitting secure data). Due to the preliminary nature of this paper, the employee-level or micro constructs were not examined.

RESULTS

Each organization was examined using the research framework. Organizations are identified as Organization AA≅, Organization AB≅, and Organization AC.≅

Organization AA≅ employs 162 employees, with approximately 55 that have Internet access. The Internet is perceived as an enhancement tool for company. The Systems Administrator routinely monitors all employees from senior management to floor shop laborers for possible Internet misconduct and misuse.

In terms of Internet e-management, the company employs the following measures to deter employee Internet abuse: flexible Internet Use Policy (disciplinary decisions at management discretion), signed employee confirmation, access control, routine and random monitoring, and implementation of firewalls to block inappropriate sites.

Job function is the primary criteria utilized to approach access control. For example, purchasing department employees are provided Internet access so they can communicate with vendors. To avoid potential sexual harassment law suits surrounding "tasteless jokes" that may be forwarded, the company mandated employees refrain from forwarding jokes. Moreover the company instituted a firewall to block inappropriate web surfing by employees and then issued a memo informing employees that they would be strictly monitored for misconduct and misuse. Employees questioned the Systems Administrator about the extent of monitoring. Some employees utilized erasing software, deleted history folders and daily email, and removed cookies to avoid detection and circumvent monitoring efforts.

Suspected cases of abuse are detected by coworker alerts, network slowdowns, abnormal amount of time spent at the computer, repeated logins, and reviewing the subject line of email. When monitoring, the IS department assesses the site content (e.g., Wrestling Mania, Autoweb, Virtual Casinos), duration at site, nature of activity (e.g., job seeking), and excessive personal use (e.g., volume of personal email, shopping, vacation planning). When incidents are detected, management initially discusses the situation with the employee.

Relative to enforcement, the company applies a philosophical approach similar to corporate drug testing such that no employee is immune from detection and possible disciplinary action. During the past year, the company gave informal reprimands to two employees for sending discriminatory or sexually

harassing email and for sending/receiving excessive personal email. In addition, one employee was terminated for job searching during work hours via the Internet.

Organization AB≅ employs 200 employees of which 75 are salaried. Approximately 60 of the salaried employees have Internet access. No shop personnel have personal computers although general-use computers have been strategically located where they can view/change personal personnel data such as 401K benefits. The company has had two years of full Internet access, provided through a corporate Intranet based in Houston, TX.

In terms of e-management, all employees are monitored although there is no formal method of monitoring. A repair person randomly scans logs and twice per week, randomly examines computer hard drives. Because the IS department reports to the comptroller, all problems are communicated to the comptroller, who then contacts HRM. The IS department is utilized to provide evidence. Lotus Notes7 history records are maintained in the event a problem occurs.

Management encourages use of the Web. Although there is no formal internal Internet use training, the organization desires Acomputer literate≅ employees. For example, solitaire is viewed as a training tool and its use is encouraged. In addition, the organization will pay tuition for employees who take computer courses to enhance their skills. Current Web uses include marketing to prospective customers/vendors, purchasing, accessing credit data through Dunn & Bradstreet, soliciting bids, obtaining software upgrades for the telephone system, and using the Web as mechanism for financial reporting. Management=s philosophical outlook regarding the Web is: AUse it wisely, but on your own time.≅

The impedance for Internet monitoring began when network performance began to deteriorate. An investigation revealed inappropriate Internet behavior as the source of the problem. As a result, a warning email was sent to employees and a formal Internet policy was adopted. The policy is not signed by the employee. At present, management is in the process of defining the reaction(s) to violators. Due the newness of the policy, the comptroller does not know whether the policy is an effective deterrent.

Relative to enforcement, four employees have received informal reprimands during the past year. The misuse included downloading or viewing online pornography, engaging in chat rooms, and stock watching during work hours. The comptroller does not view that Internet access has resulted in major problems partly because of the stability of the company=s workforce. Thus far, negative behaviors have also included chain letter forwarding and offensive joke distribution. Email is not examined.

Organization AC≅ employs 90 employees. Approximately 45 employees, mainly in administration and sales, have Internet access. The only production employees with Internet access are the quality manager, operations manager, and first shift foreman. The controller noted that it would be difficult to police use if general-use computers were placed throughout plant for production worker access. The company has both Intranet and Internet access. Full Internet access has been available for less than one year.

In terms of e-management, all employees are monitored although there is no formal method of monitoring. A proxy server is used to monitor usage. Usage samples are moved to a database which is maintained in the event a problem occurs. During the early stages of implementation, the controller did not detect much abuse and as a result, monitoring is performed infrequently. Monitoring is conducted by visual scans (as controller walks by) and through sorting a list of Web pages visited during the given week. The controller examines who and what time. Personal lunchtime access to a site such as LL Bean is permitted. When a problem occurs, the controller handles the situation with an informal note. The second step would be for the HRM manager to initiate the 1st stage of Internet policy discipline.

Management encourages the use of the Web, although there is no formal internal Internet use training. Current Web uses include electronic mail, Web searches to locate items which will be placed on manually-generated P.O.s, vendor services (freight quotes, raw material specification), and sales department usage (gather customer information). A partial electronic commerce solution will be developed in the near future.

Relative to enforcement, the organization gave one informal reprimand during the past year. Thus far, negative behavior has been in the form of joke distribution. In one instance, an email joke list was subscribed to and jokes were forwarded to other employees. The controller gave the user a warning (informally sent an email to user referring him/her to read the IAP) and blocked the site. Email is only examined if by word-of-mouth, a problem is discovered.

CONCLUSIONS AND FUTURE RESEARCH

Results indicate that Internet e-management monitoring may not be as formal as previously indicated in industry surveys. Two of the three study organizations non-systematically monitored behavior. In addition, enforcement has been limited to generally using informal reprimands, although one employee was terminated (Table 1). No formal reprimands, suspensions, or rehabilitation efforts were indicated. This may be a result of limited monitoring, the desire to maintain a stable company labor force in an environment where there is a shortage of technologically-skilled workers, and the newness of Internet behavioral problems.

The paper also demonstrates that the Internet E-Management Framework may serve as a guide for research. All organizations were examined using the macro constructs of e-management and enforcement. Although this research is exploratory, the primary weakness of the study is the limited sample size. Thus, future research needs to be directed at examining more organizations to strengthen conclusions. In addition, research needs to the conducted to examine the employee-level constructs of the framework. Overall, the framework and results will assist organizations in improving employee Internet management, maximizing productivity, limiting risk, and minimizing negative e-behavior.

REFERENCES

1. Adschiew, B. (2000). Web Workers, **NBC Nightly News**, June 24.

2. The Associated Press. (2000). Dow Chemical Fires 50 Over Offensive E-Mail, July 28. http://news.cnet.com/news/0-1007-200-2372621.html
3. Business Wire. (2000). Landmark Survey by Telemate.Net Software Shows that 83% of Companies Are Concerned With the Problem of Internet Abuse, *Business Wire*, ATLANTA, July 31.
4. Collins, L.A. (2000). Dow Chemical Fires 50 Over E-Mail, July 27. http://news.excite.com/news/ap/000727/18/dow-chemical-e-mail
5. DiSabatino, J.(2000). E-mail Probe Triggers Firings, *Computerworld*, 34:28, July 10, 1-2.
6. Fox News. (2000). Employers Crack Down on Internet Abuse, *FoxNews.com*, November 5. http://www.foxnews.com/scitech/110500/survwillance.sml
7. Greenemeier, L. (2000). 2 Billion Pages and the Web Is Still Growing, *informationweek.com*, 795, July 17, 17.
8. Seltzer, Larry. (2001). Monitoring Software, *PC Magazine*, 20:5, March 6, 26-28.
9. SR. (2000). Snoop at Your Peril, *PC Magazine*, 19:17, October 3, 86.
10. Syllabus@bdcimail.com. (2001). Internet Hosts Reach 100 Million Worldwide, *Syllabus News, Resources, and Trends Online Newsletter*, January 9.
11. Websense and Saratoga Institute. (2000). Survey on Internet Misuse in the Workplace, March , 1-6.
12. WH. (2000). Super Economy, *PC Magazine*, 19:14, August, 82.
13. Wilder, Clinton and John Soat. (2001). A Questions of Ethics, *informationweek.com*, 825, February 19, 39-50.
14. --. (2000). Net Monitoring Survey, *informationweek.com*, 805, September 25, 211.

FIGURE 1

Internet E-Management Research Framework

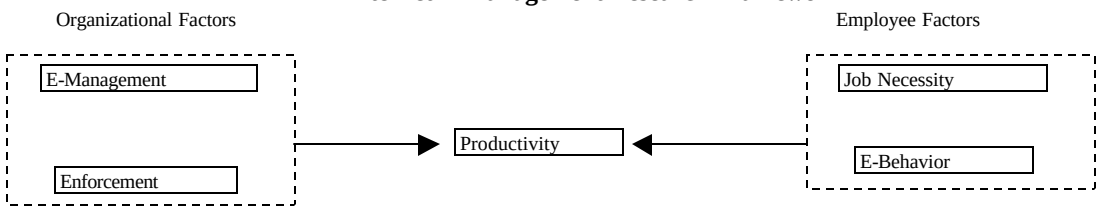

TABLE 1

Enforcement by Organization

Enforcement	Organization AA≅	Organization AB≅	Organization AC≅
Ignore the problem	0	0	0
Informal reprimand	2	4	1
Formal reprimand	0	0	0
Suspension	0	0	0
Job termination	1	0	0
Offer EAP referral and rehabilitation	0	0	0