

EMPLOYEE INTERNET MANAGEMENT: CURRENT BUSINESS PRACTICES AND OUTCOMES

Dr. Kimberly S. Young & Dr. Carl J. Case
Associate Professors of Management Sciences, St. Bonaventure University
Paper published in CyberPsychology and Behavior, 5(4), 355-361, 2002

ABSTRACT

This paper empirically examines emergent business practices that attempt to reduce and control employee Internet misuse and abuse. Over a six-month period, fifty-two web-administered surveys were collected. Respondents ranged from human resource managers to company presidents. Data were stored in a database management system and analyzed utilizing statistical measures. Monitoring efforts and policy development issues are examined against critical incidents of employee Internet abuse. The analysis also includes a rank ordering of the types of Internet applications that were perceived as most problematic or abused. Types of employee applications abused include: electronic mail, adult web sites, online gaming, chat rooms, stock trading, and so on. Moreover, company size and years online are examined. Overall, this research will assist organizations in implementing effective corporate initiatives to improve employee Internet management practices.

INTRODUCTION

As the 21st century progresses, the Internet is showing no signs of slowing in growth. Netsizer, for example, reports that there are more than 350 million Internet users worldwide.^[1] This represents a 105% increase from the estimated number of Internet users in 1999.^[2] Further evidence of the explosive growth can be found in the increase of electronic mail use. Gartner Inc. forecasts a 45% increase in the use of electronic mail for 2002, in part as a result of the anthrax attacks.^[3] Moreover, Jupiter Media Metrix Inc. of New York predicts the volume of commercial electronic mail in U.S. will triple to 424 billion messages by 2005.^[4]

The overall growth of the Internet has corresponded to an increased use by organizations. According to a Websense, Inc. survey of human resource directors, approximately 70% of companies provide Internet access to more than half of their employees.^[5] A critical aspect of usage for organizations is productivity. Users should be utilizing the Internet to increase productivity and not for non-productive uses. Dysfunctional uses include chat room participation, downloading or viewing pornography, stock watching, cybersex, and so on. Electronic mail can also be used for non-productive activities. These include sending/receiving personal electronic mail, sending harassing electronic mail, and managing spam. Spam is unsolicited bulk electronic mail and expected to consistently account for 39% of electronic mail messages each year between 2001 and 2005.^[6]

As a result, managing the corporate Internet resource may be more difficult and increasing in importance. The purpose of the current study is to utilize a research framework to empirically

examine Internet e-management practices, enforcement measures, and e-behavior. The results will assist organizations in implementing effective corporate initiatives to improve employee Internet management practices.

PRIOR RESEARCH

Prior research in the area of employee Internet management has generally been manifested in the form of industry-driven surveys. Studies have primarily examined monitoring, Internet use policies, and Internet behavior. 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, 2001) survey of 1627 managers, nearly 50% of companies monitor electronic mail, 63% monitor Internet use, and 89% monitor their employees in one way or another.[\[7\]](#) [\[8\]](#) The AMA notes that 74% of corporations use monitoring software.[\[9\]](#) Moreover, the AMA estimates that 45% of companies with 1000 or more employees monitor electronic communications from workers.[\[10\]](#) In a 2000 survey, the AMA found that approximately 38% of 2,100 major U.S. companies check their employees' electronic mail and 54% monitor Internet connections.[\[11\]](#) 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.[\[12\]](#) 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. Only 14.7% report that personal Internet use is not tolerated.

An *Information Week* research survey of 250 information technology and business professionals found 62% of companies monitor its employees' website use.[\[13\]](#) Approximately 60% monitor phone use, 54% monitor electronic mail, and less than 20% monitor productivity of home-office workers.

A Websense, Inc., study examined policies and behavior. The survey of 224 human resource management directors found that 83% of the companies indicated they have Internet access policies (IAP). Even though IAPs exist, 64% of the companies have disciplined, and more than 30% 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% of companies are not concerned about the problem and/or have done little to enforce the IAPs. 60% of the companies use self or managerial oversight and only 38% use filtering software.

Overall, studies indicate considerable employee monitoring, high incidence of IAPs, and a varying degree of discipline and termination. However, prior research has been limited to primarily industry-driven surveys. The research appears fragmented with inconclusive results and without direction. In addition, variables such as employee training, screening, and rehabilitation are not explored. Such variables would be useful in improving employee Internet

management.

INTERNET E-MANAGEMENT FRAMEWORK

The Internet E-Management Framework was developed by Case and Young.^[14] The framework was introduced to serve as a guide in analyzing Internet behavior. The framework was successfully employed in multi-site case study analysis of manufacturing firms.^[15]

The Internet E-Management Framework utilizes four constructs (Figure 1). These constructs are identified as e-management, enforcement, job necessity, and e-behavior. Each construct is hypothesized to impact productivity.

E-management and enforcement 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 practices include policy implementation, screening, training, monitoring, or no measures. Enforcement can be stated as the organization's tolerance or reaction to employee Internet misuse. Possible reactions include discipline, dismissal, rehabilitation, or no reaction.

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 electronic mail misuse (personal electronic mail, spamming, flaming, sending racist or sexual harassment electronic mail), involvement in non-work related newsgroups, chat room participation, slacking (stocks, surfing, sports, newsgroups), cybersex, pornography, gambling, and security threats (hacking, copyright, transmitting secure data).

The study employs a survey research design. A web-based survey instrument was developed by the authors and administered over a six-month period. Prior research suggests that Internet-based research studies have results comparable to postal-delivered surveys but can be administered more quickly.^[16]

The instrument was utilized to collect company demographic data and examine company Internet behavior. In terms of behavior, respondents were asked to specify Internet policies, rank order type of misuse, and detail the organization's response to Internet misuse. The survey was administered during the winter of 2000-2001. Although the surveys could be completed anonymously, 55% or 29 of the respondents included his/her name and electronic mail address in his/her survey response.

Messages were converted from ASCII format into a computer-based database management system to improve the ease of tabulation. A program was written to summarize and filter data. In addition, respondent position (i.e., manager, president, and so on) was analyzed using word or thematic content analysis. Content analysis is a qualitative research technique that uses a set of procedures to classify or categorize to permit valid inferences to be drawn.^{[17] [18]}

The Internet E-Management Framework was utilized to examine the organizations. The organization-level or macro constructs of enforcement and e-management were explored relative to each organization. Due to the preliminary nature of this paper, the employee-level construct of job necessity was not examined.

RESULTS

Results indicate that the majority of respondents are in management. 66% or 35 respondents identified himself/herself as a manager. Seven of these respondents indicated he/she is either a president or vice president.

Study demographics also provide a profile of the respondent organizations. An examination of company size indicates a relative equal distribution among size categories (Table 1). 25% of the organizations have 1-10 employees. 17% have 11-50 employees. 10% have 51-100 employees. 25% have 101-500 employees. And, 19% have more than 500 employees. Thus, approximately half of the organizations can be classified as being small (1 to 100 employees) and half of the organizations can be classified as being medium to large (more than 100 employees).

Table 2 presents a breakdown by year that the Internet was implemented into the respondent organization. 18% were implemented 1990-1995. 14% were implemented in 1996. 15% were implemented each year from 1997-1999. And, 19% were implemented in 2000. Thus, two-thirds of the organizations implemented employee Internet access within the past four years.

Responses were examined using the Internet E-Management Framework. Results were categorized using the constructs of e-management, enforcement, and predominant e-behavior. Job necessity was not studied.

E-management is the organization's culture relating to their tendency of being proactive to Internet misuse. Possible proactive practices include policy implementation, screening, training, monitoring, or no measures. Table 3 depicts e-management practices for the respondent organizations. 65% offer unlimited Internet access. 48% have an Internet Use policy in place. Only 4% employ hiring practices that screen for potential misusers. Moreover, only 19% train managers to prevent Internet misuse or abuse that effect employee productivity. 35% use monitoring software to prevent employee Internet misuse and abuse. And, only 13% indicated that his/her company controls potential Internet misuse and abuse by telecommuters. However, 87% did not answer the telecommuter question.

Enforcement can be stated as the organization's tolerance or reaction to employee Internet misuse. Possible reactions include discipline, dismissal, rehabilitation, or no reaction. Table 4 illustrates type of enforcement by response percentage. 17% maintain a zero-tolerance policy. A zero-tolerance policy would result in an immediate termination for employee Internet misuse. 33% indicate either disciplining or firing an employee(s) due to inappropriate Internet behavior. And, only 2% noted that rehabilitation was offered for Internet-addicted employees.

Predominant e-behavior includes dysfunctional behavior such as electronic mail misuse

(personal electronic mail, spamming, flaming, sending racist or sexual harassment electronic mail), involvement in non-work related newsgroups, chat room participation, slacking (stocks, surfing, sports, newsgroups), cybersex, pornography, gambling, and security threats (hacking, copyright, transmitting secure data). Table 5 presents types of e-behavior rated most problematic by respondents. Note that one respondent ranked three of the behaviors as equally problematic. The e-behaviors ranked as most problematic are personal electronic mail (abuse, harassment, inappropriate spam) and adult web sites (pornography). These e-behaviors accounted for 60% of responses and were rated at 31% and 29%, respectively. Chat rooms were ranked by 14% as being the most problematic e-behavior. Game playing and information surfing both were rated as most problematic by 10% of respondents. The least problematic e-behaviors include stock watching (4%), online shopping (4%), e-auctions (2%), and news sites/discussion groups (2%).

DISCUSSION

Results indicate that e-management measures are not implemented by most organizations. In other words, the organizational culture relating to Internet misuse is generally not proactive. Although 65% of the companies offer unlimited Internet access, less than one-half (48%) have an Internet Use policy in place and one-third (35%) use monitoring software to prevent employee Internet misuse and abuse. These results are contrary to previous industry surveys that indicate most companies have an Internet Use Policy and monitor Internet usage.

Other e-management measures further demonstrate the absence of a proactive Internet culture. Only 4% of respondent organizations employ hiring practices that screen for potential misusers. Moreover, only 19% train managers to prevent Internet misuse or abuse that effect employee productivity. And, only 13% indicated that his/her company controls potential Internet misuse and abuse by telecommuters. It should be noted that 87% of the respondents did not answer the telecommuter-monitoring question. However, none of the respondents indicated "yes" to telecommuter Internet controls. Overall, results suggest a considerable lack of e-management measures.

In terms of enforcement, results indicate that organizations are relatively lenient. Most organizations were tolerant when reacting to employee Internet misuse. Few organizations (17%) maintain a zero-tolerance policy that would result in an immediate termination for employee Internet misuse. Moreover, only 2% noted that rehabilitation was offered for Internet-addicted employees. Prior studies have not examined zero-tolerance or rehabilitative efforts.

In addition, 33% indicate either disciplining or firing an employee(s) due to inappropriate Internet behavior. Although only one-third reported disciplining or firing employees, this number is a mid-level when compared to incidences identified in prior surveys. The AMA survey found that of the organizations that monitor electronic mail and Internet connections, 17% fired employees, 26% issued formal reprimands, and 20% gave informal warnings. The Websense study found that 64% of the companies have disciplined, and more than 30% have terminated, employees for inappropriate use of the Internet.

The predominant e-behaviors identified related to personal electronic mail and adult web sites.

Personal electronic mail (abuse, harassment, and inappropriate spam) was ranked as the most problematic e-behavior by 31% of the respondents. Adult web sites (pornography) was ranked number one by 29% of the respondents. Overall, these two e-behaviors accounted for nearly two-thirds (60%) of the responses.

The remaining e-behaviors were rated as far less problematic. Chat rooms were ranked by 14% as being the most problematic e-behavior. Game playing and information surfing both were rated by 10% of respondents. The least problematic e-behaviors include stock watching (4%), online shopping (4%), e-auctions (2%), and news sites/discussion groups (2%).

In general, the ranking of e-behaviors is consistent with the Websense study. Websense found that accessing pornography was identified as the leading cause for disciplinary action or termination. The Websense study, however, did not examine electronic mail.

IMPLICATIONS

The implications of this research are important for both academics and practitioners. From an academic perspective, this study demonstrates that the Internet E-Management Framework serves as a useful guide for research. Results were examined using the organizational (macro) constructs of e-management and enforcement. In addition, the employee (micro) construct of e-behavior was studied. Overall, the framework provides a solid basis for the current and future lines of Internet management research.

From a practitioner perspective, the academic implications are instructive and should not be overlooked. More importantly, the study paints an empirical picture of current management practices and outcomes. Results indicate that e-management measures are not implemented by most organizations. This suggests a general absence of a proactive Internet culture. In terms of enforcement, results indicate that organizations are relatively lenient. Most organizations were tolerant when reacting to employee Internet misuse. Moreover, the predominant e-behaviors identified related to personal electronic mail and adult web sites. Personal electronic mail and adult web sites were ranked as the most problematic e-behaviors by nearly two-thirds of the respondents.

Results suggest that Internet e-management is in its infancy. As the Internet continues to proliferate and usage increases, dysfunctional e-behavior may become more prevalent unless e-management and enforcement techniques are formalized. In addition, results imply that education may be necessary to minimize the problems associated with electronic mail (abuse harassment, inappropriate spam) and adult web sites (pornography). Further research is needed; however, to strengthen results and provide detailed prescriptive advice for practitioners.

The limitations of this study are primarily a function of sample size and type of research. Even though responses were relatively equally distributed among organization size and number of years with Internet experience, a larger sample size would increase the robustness of results. The second limitation relates to the use of survey instruments. On-line surveys offer the researcher less control in selecting respondents. In addition, surveys provide less opportunity for the

respondent to explain his/her responses and for the researcher to further probe answers. In this survey, reliability is increased because most respondents provided his/her name and electronic mail address. Thus, researchers have the ability to verify responses and further probe respondents, if necessary.

In general, this research provides an empirical baseline of e-management practices, enforcement measures, and e-behavior. Future research is necessary to further explore potential cause and effect relationships among the three constructs. For example, what effect do various employee screening and training techniques have relative to dysfunctional e-behavior incidence and type? Moreover, future study is needed to determine the relationship of organization size and years of Internet use upon e-behavior. These variables may be moderating factors that effect e-management practices and enforcement measures. Ultimately, results will assist organizations in improving employee Internet management, limiting risk, and maximizing employee productivity.

Table 1. Organizations by Employee Size

Number of Employees	Responses	% of Respondents
1 - 10	13	25%
11 - 50	9	17%
51 - 100	5	10%
101 - 500	13	25%
501 and over	10	19%
No response given	2	4%
TOTAL	52	100%

Table 2. Year of Internet Implementation

Year	Responses	% of Respondents
1990	1	2%
1993	2	4%
1994	1	2%
1995	5	10%
1996	7	14%
	8	15%

1997		
1998	8	15%
1999	8	15%
2000	10	19%
2001	0	0%
No response given	2	4%
TOTAL	52	100%

FIGURE 1

Internet E-Management Research Framework

Organizational Factors				Employee Factors
E-Management				Job Necessity
		Productivity		
Enforcement				E-Behavior

Table 3. E-Management Practices by Response Percentage

Type	YES Respondents	NO Respondents	BLANK Respondents
Unlimited Internet Access	65%	35%	0%
Internet Use Policy	48%	52%	0%
Employ Hiring Practices That Screen For Potential Misusers	4%	40%	56%
	19%	79%	2%

Train Managers To Prevent Misuse By Employees			
Use Monitoring Software	35%	62%	3%
Control Telecommuters	13%	0%	87%

Table 4. Enforcement Practices by Response Percentage

Type	YES Respondents	NO Respondents	BLANK Respondents
Zero Tolerance	17%	83%	0%
Disciplined / Fired	33%	67%	0%
Offer Rehabilitation	2%	96%	2%

Table 5. Type of E-Behavior Rated Most Problematic

E-Behavior	% of Respondents Who Rated E-Behavior as Most Problematic
Electronic Mail	31%
Pornography	29%
Chat Rooms	14%
Playing Games	10%
Information Surfing	10%
Stock Watching	4%
Online Shopping	4%
	2%

E-Auctions	
News Sites / Discussion Lists	2%

REFERENCE

- [1]. Internet Hosts Reach 100 Million Worldwide. *Syllabus News, Resources, and Trends Online Newsletter*, January 9, 2001 ; Syllabus@bdcimail.com.
- [2]. WH. Super Economy. *PC Magazine* 2000; 19(14):82.
- [3]. Callaghan D, Gibson S. E-Biz Alternatives. *eweek* 2001; 18(18):11-14.
- [4]. Hicks M. What, Me Spam? *eweek* 2001; 18(35):51-57.
- [5]. Websense and Saratoga Institute. Survey on Internet Misuse in the Workplace. March 2000:1-6.
- [6]. Canter S. Spam, spam, spam, spam, ... *PC Magazine* 1999; 18(17):219-220.
- [7]. Swanson S. Beware: Employee Monitoring Is On The Rise. *informationweek* 2001; 851:57-58.
- [8]. Vanscoy K. What Your Workers Are Really Up To. *smartbusinessmag.com* 2001; 15(9):50-54.
- [9]. Seltzer L. Monitoring Software. *PC Magazine* 2000; 20(5):26-28.
- [10]. SR. Snoop at Your Peril. *PC Magazine* 2000; 19(17):86.
- [11]. Fox News. Employers Crack Down on Internet Abuse. *FoxNews.com* November 5, 2000 ; <http://www.foxnews.com/scitech/110500/survwillance.sml>
- [12]. -Net Monitoring Survey. *informationweek.com* 2000; 805:211.
- [13]. Wilder C, Soat J. A Question of Ethics. *informationweek.com* 2001; 825:39-50.
- [14]. Case CJ, Young KS. [Internet Risk Management: Building A Framework for Research](#). *Proceedings of the American Society of Business and Behavioral Sciences* 2001; 8(3):16-18.
- [15]. Case CJ, Young KS. [A Preliminary Investigation of Employee Internet Misuse](#). *Issues in Information Systems* 2001; 1:43-49.

[16]. Case CJ, Matz L. Internet Electronic Mail: A Viable Research Tool? Asia Journal of Business and Entrepreneurship 1998; 1(1):95-111.

[17]. Weber RP. Basic Content Analysis. 2nd edition. Newbury Park , CA : Sage, 1990.

[18]. Holsti OR. Content Analysis for the Social Sciences and Humanities. Reading , MA : Addison-Wesley, 1969.