INTERNET ABUSE IN THE WORKPLACE: NEW TRENDS IN RISK MANAGEMENT

Dr. Kimberly S. Young and Dr. Carl J. Case
Associate Professors of Management Sciences, St. Bonaventure University
Paper published in CyberPsychology and Behavior, 7(1), 105-111, 2004.

ABSTRACT

This paper empirically examines the effectiveness of emergent risk management practices that attempt to reduce and control employee Internet abuse and its potential for addiction. Over a six month period, fifty usable 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. Implementation levels of Internet use policies, management training, and clinical rehabilitation were examined and their level of perceived effectiveness to deter employee Internet abuse was evaluated. Organizational size and its impact on perceived effectiveness were also examined. This research will assist organizations in implementing effective corporate initiatives to improve employee Internet management practices. Limitations of the study and areas for future research are also explored.

INTRODUCTION

Employees who abuse Internet privileges have become a major concern among today's corporations. According to a survey of human resource directors, approximately 70% of companies provide Internet access to more than half of their employees and recent statistics show that employee Internet abuse is on the rise. In a survey of 1439 workers by Vault.com, an online analyst firm, 37% admitted to surfing constantly at work, 32% surfed a few times a day, and 21 % surfed a few times a week (Adschiew, 2000). In a survey of 224 corporations by Websense, Inc., an electronic monitoring firm, 64% of the companies have disciplined, and more than 30% have terminated, employees for inappropriate use of the Internet (Websense, 2000). Specifically, 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. In an online usage report conducted in 2000 by eMarketer.com, 73 % of U.S. active adult users accessed the Web at least once from work, 41% access the Web a majority of the time at work, and 15% go online exclusively at work (McLaughlin, 2000).

The issue has become critical as organizations attempt to minimize productivity losses that result from such employee Internet abuse, which can represent billions in lost revenue (Stewart, 2000). Vault.com estimates surfing costs $54 billion annually in lost productivity (Adschiew, 2000). For instance, in the summer 2000, Victoria's Secret posted a forty-four minute, mid-work day webcast. The broadcast had an estimated audience of two million viewers, costing Corporate America as much as $120 million. According to estimates by research firm Computer

Economics, companies lost $5.3 billion to recreational Internet surfing in 1999. Computer Economics notes that online shopping, stock trading, car buying, looking for a new house, and even visiting pornographic sites have become daily practices for about 25 percent of the workers in U.S. companies that have access to the Internet in their offices. For example, after the peak of the Clinton-Lewinsky scandals, ZDNet reported that industry experts estimated American companies lost $470 million in productivity to employees reading the salacious document online.

Telemate.Net Software, Inc., a provider of Internet usage management and eBusiness intelligence solutions conducted a study on the problem of Internet abuse in the workplace (Business Wire, 2000). Telemate.Net Software surveyed more than 700 companies from a diverse cross-section of industries. Survey respondents included executives, senior Information Technology (IT) professionals, IT and human resource managers. Findings indicated that 83% of companies were concerned with inappropriate employee usage of the Internet and the resulting legal liabilities and/or negative publicity. Over 70% indicated that employee Internet abuse results in real costs to their companies in the way of additional network upgrades, lost productivity and slow network response. The concern about Internet abuse and the associated legal liabilities, negative publicity and excessive costs was consistent across industries, company size and job titles of the respondents.

INITIAL CORPORATE RESPONSE

New electronic monitoring companies such as Websense, Spector Pro, and Cyber Surveillance have emerged in response to the problem. Features such as logging Internet conversations, web activity, screen shot capturing, and keystroke monitoring are utilized to track employee Internet usage on a daily or weekly basis. According to a 2001 American Management Association (AMA) 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 (Swanson, 2001; Vanscoy, 2001). The AMA notes that 74% of corporations used monitoring software (Seltzer, 2000). Moreover, the AMA estimates that 45% of companies with 1000 or more employees monitor electronic communications from workers (SR, 2000).

The AMA in a 2000 survey found that approximately 38% of 2,100 major U.S. companies check their employee's e-mail and 54% monitor Internet connections (Fox News, 2000). 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 (Net Monitoring Survey, 2000). 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 web site use (Wilder, 2001). Approximately 60% monitor phone use, 54% monitor e-mail, and less that 20% monitor productivity of home-office workers.

When abuse is detected, most often, employers have responded with job termination and dismissal as a means to deter employee Internet misuse. For example, *The New York Times* fired

22 employees in Virginia for allegedly distributing potentially offensive electronic mail (Associated Press, 2000). Xerox terminated 40 workers for spending work time surfing pornographic and shopping sites on the Web (AP, 2000). 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 (Collins, 2000). Merck disciplined and dismissed employees and contractors for inappropriate e-mail and Internet usage (DiSabatino, 2000).

NEW TRENDS IN RISK MANAGEMENT

While job termination may remove employees who abuse, it may create new problems with regard to increased levels of job turnover, poor employee morale, and open the door to a variety of legal liabilities (Young & Case, 2003). Recent trends suggest that lost productivity and potential corporate liability due to inappropriate Internet use can cost companies millions of dollars (Naughton, 1999). Employees may download illegal material such as copyright protected MP3 music files, pirated software, or child pornography via company computers that put the employer at legal risk. Employees may also upload illegal material to a company web server, illegally gain access to a network, or send out offensive e-mail to co-workers triggering sexual harassment claims in the workplace (Overly, 1999). Finally, a new trend has emerged under the Americans with Disabilities Act (ADA), such that employees fired based on Internet misuse, have in turn sued the company for wrongful termination based upon Internet addiction as a disability (Davis, 2003).

Over the past few years, Internet addiction has gained significant credibility as a new clinical disorder (Greenfield, 1999; Morahan-Martin, 1997; Scherer, 1997; Young, 1998, 2000). Symptoms include a preoccupation with the Internet, increased anxiety when off-line, hiding or lying about the extent of on-line use, and impairment to real-life functioning. In particular, this research has argued that addictive use of the Internet directly lead to marital discord, social isolation, divorce, and most relevant to corporations, reduced work performance and job loss. Employers are now faced with how best to respond and provide necessary resources for those suffering from the disorder. Most of all, corporations are in greater needs of ways to protect themselves from potential lawsuits.

According to the Society for Human Resource Managers, attorneys advise companies to write policies on e-mail and Internet use and electronic monitoring procedures (SHRM, 2002). They also advise employers to regularly alert employees that their online activities may be monitored and that inappropriate use may result in disciplinary action. A number of corporations rely upon Internet use policies to cut recreational use of the Internet and to mitigate legal liability regarding such misuse. For example, Websense, Inc. found that 83% of companies indicated they utilize Internet use policies in their survey of 224 corporations. Such Internet Use Policies set forth written guidelines on acceptable/ unacceptable Internet conduct and how violations will be handled.

Anecdotal evidence has shown that government agencies from NASA to the CIA and Fortune 500 companies such as US Airways and Motorola have also explored the need for clinical and

educational programs that address Internet addiction in the workplace (Young, 2002). Similar in nature to substance abuse prevention programs aimed at creating an alcohol-free and drug-free workplace, specialized management training programs have been suggested to educate supervisors on the dynamics of employee Internet abuse and its potential for addiction.

Finally, and most recently, groups such as the Employee Assistance Professional (EAPA) have seen a significant increase in self-referrals from employees who feel addicted to the Internet (Young, 2003). Employee assistance professionals and human resource managers alike have argued that Internet use policies should rely less upon restrictive zero tolerance and provide greater flexibility on ways to help employees suspected of Internet addiction seek out treatment (EAPA, 2003). Early studies show that use of direct intervention in the form of rehabilitation for employees suffering from Internet addiction will reduce employee job turnover and improve overall morale within organizational settings (Young, 2001).

Previous studies on employee Internet abuse have primarily been industry-driven and none have specifically investigated the use of rehabilitation as a means to deal with Internet abuse in the workplace. Therefore, this study examines the three new areas of risk management from Internet use policies, management training, and employee rehabilitation and their level of perceived effectiveness. The results will assist organizations in implementing effective corporate initiatives to improve employee Internet management practices.

RESEARCH DESIGN

The study employed a survey research design and administered a web-based survey developed by the authors. Prior research has suggested that Internet-based research studies have results comparable to postal-delivered surveys but can be administered more quickly (Case and Matz, 1998). Surveys were administered during the Winter of 2000-2001 and gathered company demographic profiles and addressed several relevant questions. What are current Internet use practices? What percentage of companies utilized each of the risk management strategies? Are strategies viewed an effective deterrent to curb employee Internet abuse? Is there a relationship between size of the company and perceived level of effectiveness?

Although the surveys could be completed anonymously, 55% 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 (Holsti, 1969; Weber, 1990).

RESULTS

Fifty-two surveys were collected during a six-month period but two surveys were discarded

because respondents of incomplete data. As a result, 27 (54%) came from small firms (1-100 employees), 13 (26%) from medium-sized (101-500 employees), and 10 (20%) from large firms (over 500 employees). Respondents ranged from human resource mangers to company presidents; thirty-five (70%) identified himself /herself as a manager; seven as either a president or vice-president.

Table 1 presents the current Internet use practices employed at corporations to obtain a profile of corporate cultures. Findings indicated that 60% of firms did not utilize electronic monitoring of employees, 36% did monitor, and 4% did not respond. 18% of firms employed zero tolerance with respect to employee Internet abuse while 82% did not. In terms of how firms handled situations of misuse, 34% had disciplined or fired an employee for abusing the Internet while 66% did not.

Table 1: Current Internet Use Practices

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTALS
Monitoring	36% (18)	60% (30)	4% (2)	100%
Zero Tolerance	18% (9)	82% (41)	0% (0)	100%
Disciplined/Fired	34% (1)	66% (33)	0% (0)	100%

Table 2 presents the level of implementation among the three risk management strategies. Results indicate that 50%, or half, of the organizations had instituted an Internet Use Policy and 50% did not institute such policies. Management training with respect to employee Internet abuse was utilized among 20% of the firms, 78% did not utilize training, and 2% did not respond. Lastly, rehabilitation of employees suspected of Internet addiction was the least utilized, with only 2% reporting the use of rehabilitation, or one form out of fifty, 96% did not utilize rehabilitation, and 2% did not respond.

Table 2: Implementation of Risk Management Strategies

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTALS
Policy	50% (25)	50% (25)	0% (0)	100%
Training	20% (10)	78% (39)	2% (1)	100%
Rehabilitation	2 % (1)	96% (48)	2% (1)	100%

Table 3 presents the level of reported effectiveness among the three corporate risk management strategies. Of the 25 firms that instituted Internet Use Policies, 40% found policies an effective deterrent to curb employee Internet abuse, 40% did not find policies to be effective, and 20% did not respond. Of the 10 firms that employed management training, 40% found management training to be an effective deterrent, 50% did not find management training effective, and 10% did not respond. The firm that employed rehabilitation as a means of dealing with employee Internet abuse found this approach to be effective.

Table 3: Reported Effectiveness of Risk Management Strategies

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTALS
Policy	40% (10)	40% (10)	20% (5)	100%
Training	40% (4)	50% (5)	10% (1)	100%
Rehabilitation	100% (1)	0% (0)	0% (0)	100%

Table 4 presents a breakdown of implementation based upon company size. Of the 25 companies that instituted Internet Use Policies, 36% came from small-sized firms, 36% from medium sized, 24% from large firms, and 4% did not indicate organization size. Of the 10 that employed management training to prevent employee Internet abuse, 60% came from small sized firms, 10% from medium sized, and 30% from large firms. The firm to utilize rehabilitation to address abusive or addictive use of the Internet came from a large sized firm, none from small or medium sized firms.

Table 4: Implementation by Company Size

STRATEGY	SMALL (Under 100)	MEDIUM (101 – 500)	LARGE (Over 500)	BLANK Responses	TOTALS
Policy	36% (9)	36% (9)	24% (6)	4% (1)	100%
Training	60% (6)	10% (1)	30% (3)	0% (0)	100%
Rehabilitation	0% (0)	0% (0)	100% (1)	0% (0)	100%

Table 5 presents a breakdown of reported effectiveness among small firms. Of the 9 firms that instituted Internet Use Policies, 45% found policies an effective deterrent to curb employee Internet abuse, 45% did not find policies to be effective, and 10% did not respond. Of the 6 firms that employed management training, 33% found management training and 67% did not find management training effective. Rehabilitation was not utilized among small sized firms.

Table 5: Effectiveness Rated by Small Firms

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTALS
Policy	45% (4)	45% (4)	10% (1)	100%
Training	33% (2)	67% (4)	0% (0)	100%
Rehabilitation	0% (0)	0% (0)	0% (0)	NA

Table 6 presents a breakdown of reported effectiveness among medium firms. Of the 9 firms that instituted Internet Use Policies, 22% found policies an effective, 45% did not find policies to be effective, and 33% did not respond. Of the single firm that employed management training, it was not found to be effective and rehabilitation was not utilized among medium sized firms.

Table 6: Effectiveness Rated by Medium Firms

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTALS
Policy	22% (2)	45% (4)	33% (3)	100%
Training	0% (0)	100% (1)	0% (0)	100%
Rehabilitation	0% (0)	0% (0)	0% (0)	NA

Table 7 presents a breakdown of reported effectiveness among large firms. Of the 6 firms that instituted Internet Use Policies, 50% found policies an effective deterrent to curb employee Internet abuse, 33% did not find policies to be effective, and 17% did not respond. Of the 3 firms that employed management training, 67% found management training effective and 33% did not find management training effective. The firm that utilized rehabilitation found treatment efforts to be effective.

Table 7: Effectiveness Rated by Large Firms

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTALS
Policy	50% (3)	33% (2)	17% (1)	100%
Training	67% (2)	33% (1)	0% (0)	100%
Rehabilitation	100% (1)	0% (0)	0% (0)	100%

CONCLUSIONS AND FUTURE RESEARCH

Of the three risk management strategies, Internet use policies were the most widely utilized (50%), management training was moderately utilized (20%), and rehabilitation of employees suspected of Internet addiction was the least utilized (2%). Among the firms, Internet use policies and management training were found to be moderately effective approaches (40% respectively) to curb or deter potential employee online abuse and rehabilitation was found to be an effective deterrent in the one firm which applied its use.

According to firm size, management training was the most widely utilized mechanism to deal with employee Internet abuse among small firms (60%) compared to policies (36%) and rehabilitation (0%). Among medium sized firms, Internet use policies were the most widely utilized (36%), compared to training (10%) and rehabilitation (0%). Among large firms, training was the most widely utilized (30%) compared to Policies (24%) and the only firm to use rehabilitation was by one large sized firm.

Upon further analysis, small firms found policies to be the most effective (45%) means to curb employee Internet abuse followed by training (33%) and rehabilitation was not applicable. Of the medium firms, again, Internet use polices was rated as the most effective

deterrent (22%) compared to training (0%) and rehabilitation was not applicable. Among large firms, policies were rated as the most effective (50%) followed by training (33%) and rehabilitation was found effective in the case reported.

Consistently, Internet use policies were found effective among firms, independent of organizational size, and policies offer an added benefit with respect to corporate liability to protect sizable organizations from potential lawsuits due to firings or dismissals resultant from Internet abuse. With new trends in the field of Internet addiction, employers should be encouraged to implement fair and appropriate policies to offset productivity losses caused by inappropriate use of the Internet, rather than imposing "zero tolerance" policies that alienate employees and leave the employer susceptible to litigation.

Strategies that approach Internet abuse as an addiction have been known to decrease job turnover by allowing employees the opportunity to seek treatment as an alternative to job termination (Young, 2001). Initial outcome studies report that in some cases employees are able to return to former positions without incidence of abuse and in some instances, job redesign for the employee that removes contact with the Internet has proven successful (Young, 2002). By acknowledging Internet addiction within an Internet policies program and by providing information and resources for those who may be addicted to the Internet, an employer may help to catch a problem before it gets out of control. It may also be helpful to provide a sample self-assessment to make employees aware of the signs of Internet addiction.

Furthermore, corporations that develop and implement such Internet use guidelines also need to educate employees about these company policies and clearly illustrate to employees their individual rights and responsibilities under these policies. Employers may then better utilize electronic monitoring and policy management software such as *eMinder* (Conqwest, 2003) to enforce these policies that will avoid the frustration and potential risks associated with miscommunication and misunderstanding of policies.

The rapid reliance upon the Internet has future implications on employee Internet management, especially with the proliferation of mobile computing and wireless Internet appliances. For instance, Cahners In-Stat Group report the Internet Access Devices market (which includes personal computers, mobile telephones, and smart Internet devices) is expected to grow at an annual rate of 41.6% in units from 2001 to 2005 (Abdur-Razzaq, 2002). Mobile and wireless computing will make detecting incidents of abuse even more difficult for corporations emphasizing the need to utilize an array of risk management strategies to aid in detection and prevention.

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, 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.

Future research should be directed examining more organizations to strengthen conclusions. In addition, research needs to the conducted to further examine the interaction among traditional approaches, such as electronic monitoring and zero-tolerance policies with new risk management trends to determine what facets, if any, directly relate to increasing effectiveness. Specific to management training, dynamics in terms of depth and level of training should be evaluated to evaluate long-term outcomes and effectiveness. As rapid job turnover can undermine morale, especially among those workers who are using their Internet accounts properly, proactive training and rehabilitation over termination may be especially beneficial to organizations to increase employee job satisfaction, improve worker productivity, and reduce corporate liability. Overall, the current results and future research will guide organizations in improving employee Internet management, maximizing productivity, limiting risk, and minimizing abuse of the network resources.

REFERENCES

1. Abdur-Razzaq, B. M. (2002). "Boom Times." *PC Magazine*, Volume Twenty-One, Number Five, 30.
2. Adschiew, B. (2000) "A Web Workers." *NBC Nightly News*, June 24, 2000.
3. American Library Association (2002). "Survey of Internet Access Management in Public Libraries." http://www.lis.uiuc.edu/gslis/research/internet.pdf
4. Associated Press. (2000) "A Dow Chemical Fires 50 Over Offensive E-Mail." *CNET News*. http://news.cnet.com/news/0-1007-200-2372621.html July 28, 2000.
5. Business Wire. (2000). "A Landmark Survey by Telemate.Net Software Shows that 83% of Companies Are Concerned With the Problem of Internet Abuse." July 31, 2000.
6. Case C. J., & Matz, L. (1998). "Internet Electronic Mail: A Viable Research Tool?" *Asia Journal of Business and Entrepreneurship***,** Volume One, Number One, 95-111.
7. Collins, L.A. (2000). "A Dow Chemical Fires 50 Over E-Mail." http://news.excite.com/news/ap/000727/18/dow-chemical-e-mail July 27, 2000.
8. Davis, R. A. (2003). "Internet Abuse in the Workplace." http://www.victoriapoint.com/cyberslacking.htm October 20, 2003.
9. DiSabatino, J. (2000). "A E-mail Probe Triggers Firings." *Computerworld*, 34:28, July 27, 2000, 1-2.
10. Fox News. (2000) "Employers Crack Down on Internet Abuse." *FoxNews.com*. http://www.foxnews.com/scitech/110500/survwillance.sml November 5,2000.

Greenfield, D. (1999). *Internet Addiction: Disinhibition, accelerated intimacy and othe theoretical considerations.* Paper presented at the 107th annual meeting of the American Psychological Association, August 22, 1999. Boston, MA.

1. Holsti OR. (1969). "Content Analysis for the Social Sciences and Humanities." Reading, MA: Addison-Wesley.
2. McLaughlin, L. (2000) **"**Bosses Disapprove, But Employees Still Surf.*"*

http://www.business2.com/articles/web/0,1653,15120,FF.html October 31,2000.

Morahan-Martin, J. (1997). *Incidence and correlates of pathological Internet use.* Paper presented at the 105th annual meeting of the American Psychological Association, August 18, 1997. Chicago, IL.

- Net Monitoring Survey. (2000) *informationweek.com*; 805:211.
- Scherer, K. (1997). College life online: Healthy and unhealthy Internet use. *Journal of College Development, 38*, 655-665.
- Seltzer L. (2000). "Monitoring Software." *PC Magazine,* Volume Twenty, Number Five, 26-28.
- Society of Human Resource Managers (2002). "Technology and Privacy Use." http://www.shrm.org/trends/visions/default.asp?page=0300c.asp October 2, 2002.
- SR (2000). "Snoop at Your Peril." *PC Magazine,* Volume Nineteen, Number Seventeen, 86.
- Stewart, F. (2000). "Internet Acceptable Use Policies: Navigating the Management, Legal, and Technical Issues." *Information Systems Security*, Volume Nine, Number Three, 46-53.
- Swanson S. (2001). "Beware: Employee Monitoring Is On The Rise." *Informationweek*, 851:57-58.
- Vanscoy K. (2001). "What Your Workers Are Really Up To." *smartbusinessmag.com*; Volume Fifteen, Number Nine, 50-54.
- Weber R. P. (1990). "Basic Content Analysis." 2nd edition. Newbury Park, CA: Sage
- Websense Inc, (2000). "Survey on Internet Misuse in the Workplace." March 2000, 1-6.
- Wilder C., & Soat J. (2001). "A Question of Ethics." informationweek.com, 825:39-50.
- Young, K. S. (1998) "Caught in the Net: How to Recognize Internet addiction and A Winning Strategy for Recovery." New York, NY: John Wiley & Sons, Inc.
- Young, K. S. (2001). "Managing Employee Internet Abuse: Seven Strategies to Maximize Productivity and Reduce Liability." Manual prepared for the Center for Online Addiction.
- Young, K. S. (2002). "Advanced Risk Assessment and Treatment Approaches for Internet-Addicted Clients." Workshop presented at the Employee Assistance Professional Association. November 22, 2002.
- Young, K. S. & Case, C. J. (2003). "Employee Internet Abuse: Risk Management Strategies and Their Effectiveness." Proceedings of the American Society of Business and Behavioral Sciences. Las Vegas. February 20, 2003.