EMPLOYEE INTERNET ABUSE: RISK MANAGEMENT STRATEGIES AND THEIR EFFECTIVENESS

Dr. Kimberly S. Young & Dr. Carl J. Case,
Associate Professors of Management Sciences, St. Bonaventure University
Proceedings of the American Society of Business and Behavioral Sciences,
Las Vegas, February 21, 2003, 1688-1694.

ABSTRACT

This paper empirically examines the effectiveness of emergent risk management practices that attempt to reduce and control employee Internet misuse and abuse. 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 access policies, electronic monitoring software, and management training were examined and their level of perceived effectiveness to deter employee Internet abuse was evaluated. Organizational size and its impact on implementation and 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

Over the past decade, employee Internet misuse and abuse has become a growing concern that has impacted several predominant corporations. *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).

According to a survey of human resource directors, approximately 70% of companies provide Internet access to more than half of their employees and such widespread corporate reliance on the Internet has spurred a series of industry-driven studies to investigate the prevalence of employee Internet abuse. 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.

CORPORATE STRATEGIES

As employee Internet abuse has become an identifiable concern, corporations have developed various strategies to help combat the problem. First, employers have utilized Internet Use Policies to set forth written guidelines on acceptable/ unacceptable Internet conduct. The Internet Use Policy is a visible tool that not only provides guidance on appropriate online behavior but also outlines how violations will be handled. 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 growing trend suggests that a number of corporations rely upon Internet use policies to cut recreational use of the Internet during work hours 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. Public sectors are among the most likely to utilize Internet access policies to combat abuse. In a recent study of

1,015 libraries, the American Library Association found that 94.7% have a formal written policy or set of guidelines to regulate public use of the Internet (ALA , 2002).

Second, corporations have employed the use of electronic monitoring software to deter potential abuse and to enforce existing policies. 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). In a 2000 survey, the AMA 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.

Third, anecdotal evidence has shown that government agencies from NASA to the CIA and Fortune 500 companies such as US Airways and Motorola have explored the need for clinical and educational programs to address Internet addiction in the workplace. Similar in nature to substance abuse prevention programs aimed at creating an alcohol-free and drug-free workplace, management development and training have been utilized to educate supervisors on the dynamics of employee Internet abuse to aid in prevention and early detection (Young, 2002).

Previous studies have primarily been industry-driven and have not empirically examined the level of effectiveness of these workforce practices as a deterrent to curb employee Internet abuse. Therefore, this study investigated the use and implementation of the three risk management strategies (Policies, Monitoring, and Training), their level of perceived effectiveness, and how organizational size impacted outcomes. The results will assist organizations in implementing effective corporate initiatives to improve employee Internet management practices.
the level of effectiveness of these workforce practices as a deterrent to curb employee Internet abuse. Therefore, this study investigated the use and implementation of the three risk management strategies (Policies, Monitoring, and Training), their level of perceived effectiveness, and how organizational size impacted outcomes. 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 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 the use of the strategies? Is there a relationship between size of the company and their 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 level of overall implementation among the three corporate risk management strategies. Results indicate that 48% of the respondent organizations had instituted an Internet Use Policy and 52% did not institute policies. 35% utilized electronic monitoring software and 62% did not utilize monitoring software, and 3% did not respond. 19% utilized some form of management training to detect and prevent employee Internet abuse, 79% did not utilize training, and 2% did not respond.

Table 1: Overall Implementation

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTAI
Policy	50% (25)	50% (25)	0% (0)	100%
Monitoring	36% (18)	60% (14)	4% (2)	100%
Training	20% (10)	78% (39)	2% (1)	100%

Table 2 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 18 firms that utilized electronic monitoring software, 22% found monitoring to be an effective deterrent and 78% did not find monitoring to be effective. 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.

Table 2: Overall Effectiveness

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTALS
Policy	40% (10)	40% (10)	20% (5)	100%
Monitoring	22% (4)	78% (14)	0% (0)	100%
Training	40% (4)	50% (5)	10% (1)	100%

Table 3 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 18 companies that utilized electronic monitoring software, 33% came from small sized firms, 44% from medium sized firms, 16% from large sized firms, and 7% 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.

Table 3: 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%
Monitoring	33% (6)	44% (8)	16% (3)	7% (1)	100%
Training	60% (6)	10% (1)	30% (3)	0% (0)	100%

Table 4 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 utilized electronic monitoring software, 33% found monitoring to be effective, 50 % did not find monitoring effective, and 18% did not respond. Of the 6 firms that employed management training, 33% found management training and 67% did not find management training effective.

Table 4: Effectiveness Rated by Small Firms

STRATEGY	YES R responses	NO Responses	BLANK Responses	TOTALS
Policy	45% (4)	45% (4)	10% (1)	100%
Monitoring	33% (2)	50% (3)	18% (1)	100%
Training	33% (2)	67% (4)	0% (0)	100%

Table 5 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 8 firms that utilized electronic monitoring software, 13% found monitoring to be effective and 87% did not find monitoring effective. Of the single firm that employed management training, it was not found to be effective.

Table 5: Effectiveness Rated by Medium Firms

STRATEGY	YES Responses	NO Responses	BLANK Responses	TOTALS
Policy	22% (2)	45% (4)	33% (3)	100%
Monitoring	13% (1)	87% (7)	0% (0)	100%
Training	0% (0)	100% (1)	0% (0)	100%

Table 6 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 utilized electronic monitoring software, 33% found monitoring to be effective and 67 % did not find monitoring effective. Of the 3 firms that employed management training, 67% found management training effective and 33% did not find management training effective.

Table 6: Effectiveness Rated by Large Firms

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

CONCLUSIONS AND FUTURE RESEARCH

The results indicate that Internet use policies were the most widely utilized (50%) of the three corporate risk management strategies and were found to be moderately effective (40%)

as a mechanism to deter employee Internet abuse. Management training to educate supervisors on the dynamics of employee Internet abuse was the least utilized of the three risk management strategies (20%); however this strategy was found to be equally effective (40%) to policies as a means to curb potential abuse. Electronic monitoring software was utilized among 36% of the organizations but seemed to have the least impact to curb abuse (22%).

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 monitoring (33%). Among medium sized firms, electronic monitoring software was the most widely employed (44%) compared to polices (36%) and training (10%). Among large firms, training was the most widely utilized (30%) compared to Policies (24%) and monitoring (16%).

Upon further analysis, small firms found policies to be the most effective (45%) means to curb employee Internet abuse followed by monitoring (33%) and training (33%). Of the medium firms, again, Internet use polices was rated as the most effective deterrent (22%) compared to monitoring (13%) and training (0%). Specifically, medium firms relied the most on policies and only one found monitoring effective. Among large firms, electronic monitoring software was rated as the most effective deterrent (67%) followed by policies (50%) and training (33%).

Given the mass of employees to regulate and supervise, it is not surprising that large firms reported the greatest benefit from electronic monitoring, which provides a systematic review of Internet usage among numerous employees. Electronic monitoring allows large firms to accurately track users efficiently, helping them detect patterns of abuse at an earlier stage of development. Furthermore, Internet use policies were found moderately effective among large firms 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. Interestingly, both large and small firms rated management training an equally effective deterrent (33%) suggesting that training may be a viable strategy when dealing with relatively few or relatively many employees.

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 detect and prevent abuse.

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 the three corporate risk management strategies 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 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 assist 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. DiSabatino, J. (2000). "A E-mail Probe Triggers Firings." *Computerworld*, 34:28, July 27, 2000 , 1-2.
9. Fox News. (2000) "Employers Crack Down on Internet Abuse." *FoxNews.com*; http://www.foxnews.com/scitech/110500/survwillance.sml November 5,2000 .
10. Holsti OR. (1969). "Content Analysis for the Social Sciences and Humanities." Reading , MA : Addison-Wesley.
11. McLaughlin, L. (2000) **"**Bosses Disapprove, But Employees Still Surf.*"* http://www.business2.com/articles/web/0,1653,15120,FF.html October 31,2000 .
12. Net Monitoring Survey. (2000) *informationweek.com*; 805:211.
13. Seltzer L. (2000). "Monitoring Software." *PC Magazine,* Volume Twenty, Number Five, 26-28.
14. Society of Human Resource Managers (2002). "Technology and Privacy Use." http://www.shrm.org/trends/visions/default.asp?page=0300c.asp October 2, 2002 .
15. SR (2000). "Snoop at Your Peril." *PC Magazine,* Volume Nineteen, Number Seventeen, 86.
16. Stewart, F. (2000). "Internet Acceptable Use Policies: Navigating the Management, Legal, and Technical Issues." *Information Systems Security*, Volume Nine, Number Three, 46-53.

17. Swanson S. (2001). "Beware: Employee Monitoring Is On The Rise." *Informationweek*, 851:57-58.
18. Vanscoy K. (2001). "What Your Workers Are Really Up To." *smartbusinessmag.com*; Volume Fifteen, Number Nine, 50-54.
19. Weber R. P. (1990). "Basic Content Analysis." 2nd edition. Newbury Park , CA : Sage
20. Websense Inc, (2000). "Survey on Internet Misuse in the Workplace." March 2000, 1-6.
21. Wilder C., & Soat J. (2001). "A Question of Ethics." *informationweek.com*, 825:39-50.
22. Young, K.S. (2002). "Internet Addiction in the Workplace." Paper submitted for the American Psychological Association.