INTERNET RISK MANAGEMENT: BUILDING A FRAMEWORK FOR RESEARCH

Dr. Carl J. Case and Dr. Kimberly S. Young
Associate Professors of Management Sciences, St. Bonaventure University
Published in the proceedings of the American Society of Business and Behavioral Sciences, 8(3), 16-18, Feburary 21, 2001.

ABSTRACT

The Information Systems (IS) department plays a significant role in employee Internet management. IS professionals may monitor, collect evidence, or control employee Internet use. In addition, the chief information officer may play an important role in determining corporate Internet policy. This paper will examine the current state of Employee Internet Management and its impact on productivity. In addition, a framework for future research will be presented.

INTRODUCTION - THE INTERNET PROLIFERATES

The Internet is a superhighway that is still experiencing tremendous growth. The number of users, amount of data available, and expansiveness of telecommuting are increasing at an explosive pace. The number of Internet users worldwide rose nearly 80 percent from 171 million in March 1999 to 304 million in March 2000 (WH, 2000). A portion of the growth can be attributed to the software and computer services areas. The number of employees in this arena nearly doubled from 1992 to 1998, increasing from 850,000 to 1.6 million. Another segment of the market is the general business sector. For example, over half of Honeywell's 120,000 workers are already online (Adschiew, 2000). Plans are to offer access to every employee either at the worksite or at home. 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 (2000). Moreover, the Internet is expanding in content. Cyveillance, a company which monitors pages, released a study estimating that there are 2.1 billion unique pages on the Web (Greenemeier, 2000). In addition, this total is growing by 7 million pages per day or double in volume by 2001.

Furthermore, the American Management Association telecommuting study of 1265 workers indicates increasing numbers of workers are conducting business on mobile computers (Goslar , 2000). Only 24 percent of respondents worked exclusively from the regular office location. Respondents indicated accessing company systems before and after work, while on trips, and in other business-related activities during off time. 41 percent indicated that they would rather work from home more often. The researchers indicate that the proliferation of Internet resources has likely fueled this mobility for telecommuters. Overall, the number of Internet users, either working in the office or out of the office, is growing steadily. In addition, users have more data to sort, filter, and search. Consequently, managing the employee and Internet resources is increasing in importance.

EVIDENCE OF AN EPIDEMIC

By examining the headlines, it is apparent that computer misuse is one the rise. Leading organizations such have Xerox, Dow Chemical, and Merck have not been immune. One study even surmises the cause of the problem. The New York Times fired 22 employees in Virginia last year for allegedly passing around potentially offensive electronic mail (The Associated Press, 2000). Xerox also fired 40 workers for spending work time surfing pornographic and shopping sites on the Web. According to Long Island Business News, a school principal in August forfeited three years of salary raises as punishment for viewing pictures of naked women on his office computer (2000).

In July, Dow Chemical Company fired 50 employees and suspended another 200 for up to four weeks without pays after an e-mail investigation uncovered hard-core pornography and violent subject matter (Collins, 2000). A spokesman noted that these were not instances about personal uses of the computers and "letters to mom." There was a whole range of abuses from mild pornography to very graphic pornography and seriously violent images. According to Dow, no material that could be classified as illegal was found. However, the violations were made by workers at all levels in the company. Dow's investigation was sparked by an employee complaint in May. Even though the company does not monitor e-mail on a regular basis, when officials investigated the complaint, it was determined that more than one employee was involved. The company then decided to examine all e-mail use during one week in May to get a "snapshot." Dow emphasized that the company must protect the other employees because this sort of activity creates a harassment environment that can not be tolerated.

In June, as part of an ongoing corporate crackdown, employees and contractors at pharmaceutical giant Merck & Company faced discipline, including dismissal, for inappropriate e-mail and Internet usage (DiSabatino, 2000). Merck would not indicate how many employees had been terminated or otherwise disciplined, how many employees had been subjected to e-mail and Internet monitoring or what, specifically, employees had communicated or downloaded to provoke the measures.

The problem may be more pervasive than previously surmised. According to a Reuters survey of 1,000 individuals, 54 percent of computer users get a "high" from finding information they have been looking for in an E-search (Mateyaschuk, 1997). 53 percent of these info-junkies (dataholics) crave more data, but most are overwhelmed once they are finished. A report on the survey, *Glued to the Screen*, indicates a clear link between Internet abuse, data accumulation, and information addiction.

The previous examples are primarily high-profile organizations whose stories were publicized. If these cases are representative of business in general, Internet abuse could be a silent epidemic eroding productivity for all, including the less visible organizations that dominate in quantity.

SENSE OF THE PROBLEM

Prior research in employee Internet management has been limited and primarily in the form of

industry-driven surveys. Due to the non-academic basis of study, research is fragmented with no apparent research framework in place to serve as a guide.

One study was conducted by Websense, Inc., an Internet access management company (2000). Websense commissioned the Saratoga Institute to conduct a survey on employee misuse of the Internet at work. Human resource directors at more than 1,500 companies were contacted. 224 companies completed surveys. 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%) are the leading causes for disciplinary action or termination. Percentages relate to a *yes* response to each question. For example, *Has investing resulted in reprimands or discipline over the past year?* Yes/No/Blank. Approximately 50 percent of companies are not concerned about the problem and/or have done little to enforce the IAPs (60 percent use self or managerial oversight; only 38 percent use filtering software). Pornography appears to be the clearly leading reason for discipline or reprimand. In the report, the chief executive officer (CEO) and chairman of Websense, Inc. notes that misuse of the Internet at work should never get to the point of termination (Kelsey, 2000). He suggested that companies need to start managing their Internet traffic and enforcing the Internet usage policies they already have in place. One weakness of study is that all companies were clients of Saratoga Institute. Moreover, only 15 percent completed surveys.

For the purposes of this paper, dysfunctional Internet behavior will include electronic mail and non-electronic mail World Wide Web (WWW) activities. Electronic mail misuse includes sending spam, participating in non-work related newsgroups, flaming, and sending racist or sexually-harassing electronic mail. Non-electronic mail misuse includes participating in chat rooms, slacking (stocks, surfing, sports, newsgroups), cybersex, pornography, gambling, and security threats (hacking, copyright, transmitting secure data). Sexual harassment, cybersex, and pornography will be classified as extreme negative behaviors because of their inherent legal implications.

IMPACT ON PRODUCTIVITY

Internet misuse has several impacts upon the organization. The issues relate to the drain on telecommunications bandwidth (Schoolcraft, 1999), legal liability (Stewart, 2000;Fairfield County Business Journal, 2000), security of company data (Phillips, 1999), and ultimately lost productivity. The focus of this paper will be upon productivity.

According to the U.S. Department of Commerce's "Digital Economy 2000" report, the digital economy is now the driving force of the overall economy (WH, 2000. The U.S. annual productivity growth rate of 1.4 percent from 1973 to 1995 rose to 2.8 percent after 1995. The Council of Economic Advisors, the Congressional Budget Office, The Federal Reserve, and outside economists credit information technology (IT) with at least half of the acceleration in U.S. productivity growth rate.

However, in a September 1999 survey of 1439 workers by Vault.com, 37 percent admit surfing constantly (Adschiew, 2000). 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. Webcast productivity losses are also present. The summer 2000 Victoria's Secret 44 minute, mid-work day webcast had an estimated audience of 2 million viewers, costing corporate America as much as $120 million.

The potential negative impacts from lost productivity alone represent a multibillion dollar issue for today's companies (Stewart, 2000). 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 conducted the research study via the Internet and surveyed more than 700 companies from a diverse cross-section of industries. Survey respondents included executive, senior IT, 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. 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.

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

INTERNET RISK RESEARCH FRAMEWORK

As a result of previous study results and case study interviews, the following Internet E-Management Framework is introduced. Four constructs, identified as enforcement, e-management, job necessity, and e-behavior, are presented and hypothesized to impact productivity (Figure 1). In addition, risks are identified relative to each construct.

Enforcement and e-management are organization-level or macro constructs. 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. 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.

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) (Figure 4).

The constructs can be examined through two Internet Management Matrices. The first matrix details the organization or macro management level regarding employee Internet use (Figure 2). Enforcement is plotted versus e-management. Enforcement (x-axis) is a measure of tolerance in the event of misuse. The extremes include 100 percent enforcement (zero tolerance - action is taken) versus 0 enforcement (100 percent tolerance - free use). E-management (y-axis) is a measure of management's position prior to the event of misuse discovery. The extremes include no management to overt/covert measures that result in employee termination. A Corporate Culture Assessment instrument is being developed to measure these two dimensions.

The second matrix details the employee behavior usage/incident or micro level (Figure 3). Job necessity is plotted versus predominant e-behavior. Job necessity (x-axis) is a measure of how much the Internet is required for the employee to fulfill his/her job's functional requirements. The extremes include unnecessary (zero necessity) to 100 percent necessary. Necessity can be calculated by dividing Internet required hours by total productive hours. E-behavior (y-axis) is a measure of the employee's predominant dysfunctional Internet behavior. The extremes include entertainment such as stock-checking to threatening behaviors such as cybersex or sexual harassment.

Risk is defined as the likelihood of misuse. Risk is related to the productivity of both the organization and individual employee. At the organizational level, if enforcement is high and e-management is high, then the productivity risk is low. If enforcement is low and e-management is low, the risk may be high. At the employee level, if job necessity is low and e-behaviors are in entertainment realm, then the productivity risk is low. If job necessity is high and e-behaviors are threatening, the risk may be high.

Internet e-management can be further explained as a range or continuum of approaches (Figure 5). Management can approached from the extremes of a proactive perspective to a reactive perspective. Four management behaviors include practices relating to hiring, prevention, enforcement, and termination/rehabilitation.

Hiring includes screening prospective employees for Internet misuse tendencies. Screening could be in the form of a survey instrument or interview.

Prevention includes use of policies, education/training initiatives, sensitivity training, and coaching. Policy behavior includes policy development, communication, acknowledgment, and reinforcement. Sensitivity training may utilize small group exercises of dilemmas, brainstorming

for high risk work environments, and so on.

Enforcement examines the technological infrastructure. Aspects include monitoring, filtering, and detection. Monitoring examines who is monitored, power issues, firewalls, and security. Detection can examine statistics related to number of pornographic sites visited.

Termination/rehabilitation examines the effects of firing or rehabilitation. Of interest are the legal implications of termination and the potential loss of an otherwise productive employee.

The Internet E-Management Framework create a guide for study. The Management Matrices can be utilized to determine potential risk. Result can be used in conjunction with the E-Management Approaches to determine a course of action. For example, if both the organization and employee matrix are in the high risk areas, then more facets (aspects) of the Internet E-Management Approaches should be implemented.

The research framework is important from both the academic and practitioner perspectives. From an academic standpoint, the framework is useful in providing research direction in a presently fragmented area. From a practitioner-orientation, results may be used to improve employee Internet management to maximize productivity, limit risk, and minimize negative behavior.

CONCLUSION

This paper has examined the current state of employee Internet management. The Internet size and number of users are increasing at a dramatic pace. As a result, employee Internet management is becoming more critical as organizations attempt to minimize productivity losses. Current research has been industry-driven surveys and without an apparent framework. This paper introduces an Internet Management Framework to serve as a guide for research. The framework is utilized to develop two management matrices. One matrix examines management at the organization level. The second matrix examines management at the employee level. An E-Management Approach continuum is also presented. In general, case study and further research studies are necessary to improve the strength of the framework and matrices. Both practitioners and academics are likely to benefit greatly from this research.

BIBLIOGRAPHY

Adschiew, Buba. "Web Workers." *NBC Nightly News*, June 24, 2000 .

The Associated Press. "Dow Chemical Fires 50 Over Offensive E-Mail. http://news.cnet.com/news/0-1007-200-2372621.html July 28, 2000 .

Business Wire. "Landmark Survey by Telemate Net Software Shows that 83% of Companies Are Concerned With the Problem of Internet Abuse." Business Wire, ATLANTA , July 31, 2000 .

Collins, Lisa A. "Dow Chemical Fires 50 Over E-Mail."
http://news.excite.com/news/ap/000727/18/dow-chemical-e-mail
July 27, 2000 .

DiSabatino, Jennifer. "E-MAIL PROBE TRIGGERS FIRINGS."
Computerworld, 34.28, July 10, 2000 :1-2.

Fairfield County Business Journal. Free assessment identifies workplace Internet abuse."
Fairfield County Business Journal 39.6, February 7, 2000 :18-20.

Gillham, Chris. "Practical solutions." *St. Louis Business Journal* 20.23,
February 14, 2000 :15.

Goslar, Martin. "The New E-Security Frontier."
informationweek.com 794, July 10, 2000 :67-73.

Greenemeier, Larry. "2 Billion Pages and the Web Is Still Growing."
informationweek.com 795, July 17, 2000 :17.

Kelsey, Dick. "Most Employees Disciplined For Internet Abuse."
News Bytes News Network, January 22, 2000 .

Mateyaschuk, Jennifer. "New drug of choice." *InformationWeek* 661,
December 15, 1997 :14.

Phillips, Tim. "The enemy within." *Director* 54.8, March 1999:89.

Schoolcraft, Lisa R. "E-mail, Internet abuse can create hostility in workplace."
Business Journal: Serving Jacksonville & Northeast Florida 14.31,
May 7, 1999 :26.

Stewart, Farley. "Internet Acceptable Use Policies:
Navigating the Management, Legal, and Technical Issues."
Information Systems Security 9.3, July/August 2000:46-53.

Websense and Saratoga Institute. "Survey on Internet Misuse in the Workplace."
March 2000:1-6.

WH. "Super Economy." *PC Magazine* 19.14, August 2000:82.

Employers grapple with Internet abuse at work. *Long Island Business News* 47.35, September 1,
2000 :21A