CYBERSLACKING – LEGAL AND ETHICAL ISSUES FACING IT MANAGERS

Dr. Beverly Oswalt, Southern Arkansas University, bjoswalt@saumag.edu
Dr. Florence Elliott-Howard, Stephen F. Austin State University, felliotthoward@sfasu.edu

ABSTRACT

This paper explores legal and ethical issues facing IT managers concerning the unauthorized personal use of the Internet on the job (cyberslacking). Information Systems students must be made aware of the issues concerning cyberslacking, and they must learn how to develop and implement policies and procedures that will help minimize the impact on employee productivity, employer liability, company security, and company resources. Information Systems students will have a clearer understanding of the legal and ethical issues related to cyberslacking when the information discussed in this paper is taught in the classroom.

Keywords: cyberslacking, Internet abuse, legal and ethical issues, email policies

INTRODUCTION

Internet access in the workplace causes multiple concerns for employers, including productivity, legal liability, security threats (3)(13)(2) and drain on computing resources and bandwidth (20). Employers are concerned about lost productivity because it affects the bottom line and impairs business efficiency and customer service.

They also look at the problem of cyberslacking from a liability and legal perspective knowing they could be held responsible for employee conduct while using the Internet. Security is also a concern, with fears ranging from loss of trade secrets and breach of confidentiality to breach of network security. Cost of computing resources dramatically increases when unauthorized use of the Internet puts a heavy demand on computing resources and bandwidth.

Employee Productivity

Cyberslacking is costing millions of dollars in lost productivity each year. U.S. Treasury Department monitoring discovered that over half of the Internet use by IRS employees was for personal reasons. Another study found that visits to pornography sites during the 8-5 workday accounted for almost 3/4 of all visits to pornography sites (19). "On the average, non work-related surfing costs American businesses $54 billion and 30%-40% in productivity losses every year" (22).

In a study of online shopping during September and October 2002, AOL and RoperASW found that 43 percent of people take time from their workday to shop (19). A web surfing report by Websense found that 70% of Net surfing is done at work (17). Another survey examining computer use showed that, in a single month, the collective employees of three companies spent the equivalent of 350 eight-hour workdays accessing the Penthouse Magazine Web site (14).

"Reasonable employers expect workers to handle *some* personal chores on the job", says Lewis Maltby, president of the National Work Rights Institute (3). Stewart (20) agrees, "...organizations that provide their employees with Internet access expect that there will be some small amount of personal use." But, in many instances, "some" personal use turns into hours of lost productivity. The typical employee doesn't intentionally violate workplace rules.

Unfortunately, there are web sites that feed employees with the notion that cyberslacking is OK as long as they can get away with it. One site (www.ishouldbeworking.com) provides a panic button to instantly replace your game board or other non-work related web site with a business site if you see the boss looking your way! Visitors to that site are welcomed with the banner, "Welcome Slackers." Don's Boss Page (www.donsbosspage.com) opens with a spreadsheet at the top and displays, "Spreadsheet_2001.doc" in the title bar just in case someone is observing your visit to that non-work related site.

Employer Liability

"Liability for passing inappropriate content can be a bigger threat to the health of a business than a security threat such as denial-of-service attack. Liability might occur in areas such as: breach of copyright, breach of confidentiality, loss of commercially sensitive information, and employee harassment." (25). A number of recent cases have allowed the possibility of the employer being held liable for acts of employees.

In the case of Owens vs. Morgan Stanley & Co. (16), a federal district court in New York held that a group of black employees could sue their employer for discrimination and retaliation following their complaints about racist jokes in an internal email message. Chevron Corporation paid $2.2 million in 1995 to women employees to settle a sexual harassment lawsuit based on dirty jokes sent through office email (24).

The U.S. Supreme Court has ruled, "Companies now must exercise reasonable care to prevent as well as promptly correct any sexually harassing behavior." The Australian Human Rights and Equal Opportunity Commission (HREOC) states, "Managers are responsible for monitoring work environments and ensuring that acceptable standards of conduct are observed." (24). The Telecommunications Act of 1996 (23) includes a provision to relieve an employer of liability if use of its computer network is regulated in a way that makes clear that harassing or otherwise objectionable email will not be tolerated.

In addition to possible liability for acts committed by employees against other employees, the employer also has potential exposure to liability for illegal online activities by an employee in the workplace. The common law legal doctrine of *respondeat superior* may allow an employer to be held liable for the wrongful or illegal acts of its employees committed within the scope of employment. However, because the law has not kept up with technology in the regulation of unlawful online activities, both federal and state statutes and the courts have expanded the situations in which employers can be held liable for illegal acts of employees. Cases involving wrongful death caused by drunk driving on the job, sexual assault committed in the workplace, and rape of a customer by a deliveryman have made clear that the courts are willing to hold employers liable even when the employee's act had no purpose of serving the employer. Illegal

online activity by employees can result in liability for employers in cases involving securities fraud through manipulation of stock prices, "cybersmearing" from posting false and damaging statements over the Internet, copyright infringement based on illegally copying or transmitting copyrighted material, trademark infringement and misappropriation of trade secrets, damage caused by computer viruses and worms introduced from the workplace into electronic commerce by an employee, and Internet gambling using the employer's computer equipment (12).

New York Life (Meloff v. New York Life) was sued for defamation and libel. The suit alleged that circulated email accused the employee of fraud (24).

Company Security

"...[T]he Web provides employees with the temptation to spend their time and use the resources for non-business ends. Controlling Internet usage is only one aspect of the e-business security issue, but it is one that is important to all businesses." (25). It is essential that companies use email filtering to help thwart security threats. Products such as SuperScout by SurfControl can examine email for potential Trojans or viruses. Email filtering rules can be used to support a company's confidentiality policy and help prevent the lost of confidential information. Alarming statistics warn of the magnitude of the problem.

A senior financial analyst at Lockheed Martin opened an email attachment expecting to find a blank template. Instead, she found proprietary rate calculations from a competitor. She immediately alerted her boss and legal counsel and the IT department removed the document from the server, stored it on disk, and returned it to the competitor (26). This is a reported case where the parties involved were honest. How many other incidents occur daily that go unreported?

Company Resources

Drain on company resources can include many factors, including leaked confidential information, staff replacement, financial impact, financial drain, security costs, and legal costs. (24).

It is estimated that 10%-20% of network traffic is non-work related (15). A SurfControl study found "73% of U.S. workers who use the Internet for non-business surfing are fully aware they are consuming valuable bandwidth and hampering mission-specific Internet use" (22).

Instant Messaging (IM) is the latest cyberslacking habit that is draining company resources. Analysts estimate that IM accounts for 60% of all messages sent (2).

"Efficiency is impaired when corporate resources are diverted from business uses to non-business uses. The most serious impact of this is when an employee's non-business use of the facilities gets in the way of business use, resulting in degraded customer service or in a reduction of the productivity of other employees." (25)

RAISING AWARENESS OF LEGAL AND ETHICAL ISSUES

IT managers must be particularly aware of the legal and ethical issues concerning the use of the Internet on the job. IS students must develop a solid background in the ethical use of the Internet and, as IT managers, be willing to enforce company policies and procedures.

The Internet is a powerful distraction and there is a fine, ethical line between the use and abuse of the Internet on the job. There is a blurring line concerning where work is done. If an employee uses their home Internet connection for work purposes, why can't they use their work Internet connection for home or personal use purposes? What about the mobile employee who has access to a company owned PDA or laptop 24 hours a day–where is the line drawn?

David Gebler, Working Values Group, a consulting firm that develops ethics training programs for major corporations, says that the old thinking of "ethics is nice, but let's get back to work,"' doesn't work in today's business context. "E-business raises ethical issues that may have existed before, but not in such stark reality." (26)

A survey by PC World Online found that over 65% of employees agree that their employer has the right to monitor but almost 95% said that they should be informed first (4). The courts seem to be willing to allow employer review of email both when an employee has agreed not to use email for non-company purposes and then sends personal messages over the company system and when the employer promised not to intercept email or to terminate an employee based on its contents and then read email and fired the employee. The lack of a reasonable expectation of privacy has been the key element cited by these courts and others in allowing employers to monitor and read employees' email. (5).

Increasing use of information technology requires that employers protect vital information. This need should not be allowed to override all ordinary expectations that employees have about their privacy in the workplace. While digital technology gives employers some very intrusive ways to conduct workplace surveillance, an employment relationship does not open an employee's entire life to the employer's scrutiny. It is important to require that all surveillance technologies, operations, and practices to be subject to accountability and specific criteria be used in deciding targets and use of data obtained (6).

Establishing written policies and offering employee training on those policies will help educate employees and raise ethical awareness of employee and employer issues related to Internet acceptable use policies (20).

Written Policies

Ira G. Rosenstein, partner in Orrick, Herrington, & Sutcliffe, as quoted in Information Systems Security, states, "the Internet is a valuable tool and therefore it is very important to craft the usage policy in such a way that it reinforces productivity and employee morale, without becoming unmanageable." Policy inflexibility can hinder a proportionate response. "Legalese" has its place, but Internet use policies need to be understood by all managers and employees. Written policies must be clear (20). "Setting corporate limits on Internet use can be an

emotionally charged subject, linked as it is to issues of personal privacy and individual responsibility." Top-down policy making must be avoided and developing Internet use policies should be a team effort (4).

According to Mark Grossman, an attorney specializing in computer and e-commerce law, "A well-drafted acceptable-use policy (AUP) will address such issues as computer system integrity and security, employee productivity, preventing legal liability from sexual harassment claims, copyright infringement, defamation and protecting trade secrets" (10). If the AUP provides for monitoring of employee computer use, the employer should actually monitor use. The failure to implement the full policy might allow an employee to claim that such a failure allowed the employee's expectation of privacy to be restored (8). In drafting a policy, consideration should be given to the fact that privacy laws are different from state to state and the recognition that this area of the law is still developing (10).

Stiefer suggests points to consider in drafting Internet use policies. The policy must clearly state how far-reaching the policy will be, the issues related to ownership of email, the extent to which email can be used for personal communication, a clear definition of offensive or inappropriate email, the extent to which employees can send confidential or sensitive information, a clearly defined list of acceptable and unacceptable email sites, and policies concerning downloading files (21).

Writing the Internet use policy is the first step toward curbing the tide of cyberslacking. But, just writing the policies is not enough. Companies must also invest in employee training.

Employee Training

Lookheed Martin requires its 100,000+ employees to complete an hour of ethics training every year. "Our goal is to raise awareness, to be proactive and preventive rather than punitive", says Tracy Carter Dougherty, Lockheed Martin's director of ethics communication and training (26).

Dianah Neff, deputy city manager and CIO for San Diego, describes their email and Internet use training for its employees and officials as a two-hour quarterly session. In addition, a PowerPoint presentation is available on the city's Intranet and an email etiquette video change be checked out for viewing at any time (1).

In the "Top 10 Principles for Positive Business Ethics" published by Philip Humbert in the TIP's Letter, the first principle is that business ethics are built on personal ethics. "There is no real separation between doing what is right in business, and playing fair, telling the truth and being ethical in your personal life." (11)

Friedman suggests that training has to be structured to help employees avoid placing themselves in the child mode of trying to get away with something until caught (7). Dr. Kimberly Young, executive director of the Center for Online Addiction in Bradford, Pennsylvania, believes that employers should acknowledge Internet addiction and should establish a means of informing employees about its warning signs (9).

CONCLUSION

IT managers must grasp the seriousness of the legal and ethical issues that cyberslacking brings to the workplace environment. Reduction of cyberslacking will help prevent lost employee productivity, reduce employer liability, improve company security, and minimize the drain on company resources.

An open dialogue and increased employee training, presenting both the employee and employer side of the issues, will increase awareness and help employees personally define the legal and ethical line between use and abuse of the Internet. Written and enforced company policies concerning Internet use will establish clear, ethical boundaries and allow employees to personally determine what needs to be done to abide by such policies.

Information Systems students will have a clearer understanding of the legal and ethical issues related to cyberslacking when the information discussed in this paper is taught in the classroom.

REFERENCES

1. Bowen, D. and Gold, B. (2001). Policies and education solve e-mail woes. *American City & County, 166(7).*
2. Bowman, L. M. (2002, December 4). Drinking at the virtual water cooler. *CNet*.
3. Brauer, D. (2001). Somebody's watching you: The office walls may have eyes and ears. *My Generation*.
4. Developing a corporate Internet access policy. (2001). SurfControl, Inc. Retrieved from http://www.surfcontrol.com/news/white_papers/industry/index.html
5. DiSabatino, J. (2001). E-mail probe triggers firings. *Computerworld*, *34(28).*
6. Dixon, R. (1999). With nowhere to hide: Workers are scrambling for privacy in the digital age. *Journal of Technology Law and Policy.*
7. Friedman, W. H. (2000). Is the answer to Internet addiction Internet interdiction? *Proceedings of the 2000 Americas Conference on Information Systems,* 1564.
8. Garvey, C. (1999). The new corporate dilemma: Avoiding liability in the age of Internet technology. *Dayton Law Review*, *(25)*, 133-162.
9. Greengard, S. (2000). The high cost of cyberslacking. *Workforce, 79(12)*, 22-24.
10. Grossman, M. (1999). Drafting an acceptable computer-use policy: Protecting employers from liability due to employee misuse of e-mail and the Internet. *New Jersey Law Journal*, *157*, 1005 ff.
11. Humbert, P. (2001). Top 10 principles for positive business ethics*. TIP's Newsletter.* Retrieved from http://www.philiphumbert.com
12. Ishman, M. (2000, Spring). Computer crimes and the respondeat superior doctrine: Employers beware. *Boston University Journal of Science and Technology Law.*
13. Jackson, W. (1999). Legal liability of web access a top concern. *Government Computer.*
14. Nichols, D. H. (2001) Electronic commerce in the 21st century: Window peeping in the workplace: A Look into employee privacy in a technological era. *William Mitchell Law* Review, 27(1587), 1592.
15. Olsen, S. and Bowman, L. (2003, January 24). Office surfers may face wipeout. *CNET News.*

16. Owens v Morgan Stanley & Co., 1997 U.S. Dist. LEXIS 20493 (S.D.N.Y. 1997).
17. Palmer, A.T. (2001, July 11). Workers, surf at your own risk. *Business Week*, *3736*,14.
18. Richtel, M. (2002, December 24). Net shoppers log on from work. *New York Times*.
19. Schwabach, B. (2001, July 23). Jobs aren't getting done? Workers likely on net. *Arkansas Democrat-Gazette*, 1D-2D.
20. Stewart, F. (2000, July/August). Internet acceptable use policies: Navigating the management, legal, and technical issues. *Information Systems* Security, 9(3), 46-52.
21. Stiefer, S. L. (2000, March/April). Developing sensible e-mail and Internet use policies. *Assessment Journal, 7(2)*, 53-56.
22. Surfing the web at work: Corporate networks are paying the price. (2000). Retrieved from http://www.surfcontrol.com/news/white_papers/industry/index.html
23. Telecommunications Act of 1996. 47 U.S.C. 502(e)(4), 502(e)(5), 502(f)(1).
24. The business case for email filtering. (2001). SurfControl, Inc. Retrieved from http://www.surfcontrol.com/news/white_papers/industry/index.html
25. The role of information filtering in raising business efficiency. (2001). SurfControl, Inc. Retrieved from http://www.surfcontrol.com/news/white_papers/industry/index
26. Wilder, C. and Soat, J. (2001, February 19). A question of ethics. *InformationWeek.*