Putting the Lid on Pandora's Box

BAJAI

www.bajai.com

Suite A 1647 Bank St. Ottawa, Ontario, K1V 7Z1 Canada 613-731-9069

I - Introduction

The Internet can boost productivity by enhancing communications, collaborations and research capabilities in the workplace. However, it can also undermine efficiency should users spend too much time surfing for personal reasons. It doesn't take many employees downloading MP3s or movie trailers to clog networks, and it takes only one employee accessing sexually explicit material to embroil an organization in an expensive lawsuit.

According to a study by the University of Texas, the Internet was responsible for pumping an estimated $507 billion into the U.S. economy during 1998. The explosion of the Internet has undeniably transformed the way business is conducted. Information from anywhere in the world can be retrieved instantly from the office.

However there is another side to the Internet. Employees can now take care of personal business while on the job - paying bills, making travel arrangements, trading stocks, shopping for gifts, and playing games. Therein lies the Pandora's box for employers, Human Resources Departments and IT managers. Research in this area revealed the following:

- 37% of employees constantly surf the web at work for personal reasons. (Vault.com)
- 57% of employees feel that surfing the Internet or sending non-work related e-mails decreases productivity. (Vault.com)
- Up to 800 million business hours will be wasted in Canada this year by employees using the Internet for personal reasons. (Ipsos Reid)

The price tag attached to this lack of productivity is enormous. According to DVD Software, business and government agencies lose an estimated $52 billion a year in productivity due to *online games alone*. That cost triples when other non-work related Internet activities are added into the mix, such as entertainment, shopping, stock trading etc.

Another issue to consider is a company's network resources. A major public relations firm banned the use of Napster, the controversial site that allows users to download music, when it found that the virtual jukebox was eating up 80% of the company's bandwidth. Downloading audio and video can consume a minimum of 50% to 60% of a company's bandwidth, seriously impacting legitimate Internet business.

Furthermore, the sites employees access while at work are also cause for alarm. Pornography, racism, hate groups and other offensive material can lead to a hostile work environment and put a company on thin ice if it offends a co-worker. Several surveys indicate that accessing offensive Internet material is becoming more widespread.

- 27% of Fortune 500 companies have defended themselves against claims of sexual harassment stemming from inappropriate e-mail and/or Internet use. (AMA)

- US-based Yankelovich partners found that 62% of workers go online at work for personal reasons at least once a day, while about 20% do so 10 or more times a day.
- According to Sextracker.com, 70% of the pornographic traffic happens during 9-5.

Companies should be concerned about this growing problem. The risks are increasing and companies are beginning to take action.

- In a recent survey by Strategic Surveys International of Fortune 500 companies, more than 60% who responded had disciplined or fired employees due to inappropriate Internet activities.
- PC magazine found that one in five companies had disciplined employees due to improper Internet usage.
- The New York Times, First Union Bank and Xerox have fired employees for sending offensive messages on the company's e-mail system.

It is clear that misuse, big and small, happens everyday. Less clear is what companies should do. On the surface, the answer seems easy: install activity management software; but there is another side to the issue. For example, what exactly should be blocked? Sexually explicit sites are the most obvious, but what about shopping sites? Maybe it's not such a bad idea for someone to take five minutes to buy a battery for a company laptop or shop for a co-worker's gift at Amazon.com rather than going out of the office for an hour.

The challenge is to create a usage policy to guide the administration of the online activity management (OAM) software, which protects your business without causing turmoil among your employees.

II - Creating Policy

The first step to managing the Internet in the workplace is to establish an Internet Usage Policy. At minimum the policy should define the intended use of the provided resource. State your organization's position on usage and enforcement. To help clarify these issues you can answer the five "W"s: who, what, when, where and why.

Which individuals or groups in your organization need Internet access? Does the mail room staff need Internet access? How about the marketing or accounting departments? Once *who* needs access is determined, then *what* services are necessary for each individual or group (i.e., e-mail, file transfer, browsers, data base access etc) must be decided. Does an essential business application have to be Internet enabled? When you know *who* and *what,* then *when* can be addressed. Do they require full access, access to work-related sites only, or periodic access to other sites, perhaps during lunch hours? The next decision is *why* they need access. The last issue is *where* they need access; for example, on a laptop for business trips, in the office or at home.

Be realistic when establishing a company policy. Start with the obvious restrictions: no adult sites, no racial, social or gender harassment. Compare Internet usage to current practices. If employees are used to bringing newspapers to work, would you disallow news sites? The policy should reflect your organization's fundamental work ethics.

The policy should be included in the employee manual and signed during employee training. It should establish permissible use of the company's resources to access the Internet. A policy often includes:

- A precautionary disclaimer that informs employees about objectionable content on the Internet and protects employers from liability if that content is viewed.
- An outline of limitations that describes the appropriate use of network resources (i.e., no personal or commercial use, no communication of confidential company materials and information, etc)
- A waiver of rights of privacy, which informs employees that all material accessed and used via the company's Internet belongs to the company and is available for the company to view, log, monitor and/or block.
- An agreement that improper or illegal use of the company's Internet resources infringes on work time and can cause network and server congestion as well as negative publicity or legal liability.

A policy eases employee tension with regards to cyberslacking and harassment, thereby promoting a healthier work environment. Of course, an acceptable usage policy is most effective when actively promoted and consistently enforced.

III - Educate

Keep the policy simple and easy to understand. Once it has been established, provide a clear, precise summary. Educate current and new employees via seminars, memos and personal coaching and have everyone sign the policy. Send out regular updates and explanations of any changes to policy or enforcement. Inclusion makes everyone feel more comfortable. When you update the policy, update the learning as well.

IV - Enforce the Policy

Enforcing the policy is also important. Corporate liability is reduced when employees are reminded that the company is committed to the policy and its guidelines.

Online Activity Management software and reporting tools ensure that employees are in compliance with the acceptable usage policy. Businesses who have implemented a policy along with activity management tools have reported significant improvements in their network speed. Employees are more productive and the risk of legal liability has been reduced. Reporting tools document the use of the company's Internet resources. Use OAM software that prevents employees from accessing objectionable or non-work related Internet material. These programs can be customized to block certain sites from individuals or departments.

The company's Internet usage policy should establish a graduated system for dealing with infractions. First would be a verbal or written warning. Continuing violations would lead to withdrawal of Internet privileges, then suspension and finally, dismissal.

Do not be secretive about the OAM software. The company is not censoring; it is providing a resource and ensuring its use in the safest and most reasonable manner.

V – Support for the Enforcement

The IT staff may be perceived as the "bad guys" and will need to be supported. Everyone needs to know that this is COMPANY policy. Hiring a third party to assess user logs can reduce the stress of having co-workers ask to be exempt from policy enforcement. OAM companies, aware of this issue, often offer this service for a minimal cost.

The IT staff should be fully informed about the legal and interpersonal issues that were considered before the policy was instated and enforced. Confidential support systems should be in place to assist them.

VI – Keeping Current

Employees should be continually educated about the importance of security and why online activities are monitored. Discuss bandwidth management and anti-virus measures in addition to legal issues. Frequent reminders in newsletters and communications will ensure a continued awareness of the Internet usage policy. These should also outline the disciplinary actions in the event that policy is violated.

Regular review of the company's policy will help to maintain consistent enforcement. The policy should be adapted to reflect new Internet trends and technology, and employees must always be informed of any changes.

Ensure that your OAM technology is up to date and capable of enforcing any new policies. Use OAM software that is adaptable and will allow you to implement any changes in a timely manner

VII - Conclusion:

The Internet is a wonderful tool that can have positive effects on your working environment. But having such a powerful tool in the office can and does lead to inappropriate use. A company that does not have an Internet usage policy leaves itself open to reduced productivity and potential lawsuits. An organization that has a policy but is not following up with enforcement is also at risk. The key to a successful Internet policy is to employ it with an online activity management tool that keeps up to date with the ever-changing world of the Internet.

Disclaimer:

Due to the legal liabilities associated with Internet misuse and the variations in laws from province to province and country to country, you should have a lawyer examine your Internet usage policy.