# Monitoring Strategies for Internet Technologies

**Andrew Urbaczewski**
*University of Michigan, Dearborn, USA*

## INTRODUCTION

Most large organizations that provide Internet access to employees also employ some means to monitor and/or control that usage (Reuters, 2002). This article provides a classification and description of various control mechanisms that an organization can use to curb or control personal Internet usage. Some of these solutions are technical, while others rely instead on interpersonal skills to curb cyberslacking.

After a review of goals for a monitoring program, a list of different activities to monitor and/or control will also be provided. Then a discussion of different techniques for monitoring and associated products will be explored, followed by a discussion of fit between corporate culture and monitoring.

## BACKGROUND

### The Worker's Perspective

In this age of cell phones, pagers, wireless PDAs, email, and home network links, many employees feel like the employer owns them not just during the workday, but perhaps constantly. Though tiresome, the worker may accept this as an unfortunate circumstance of 21st century knowledge work. However, in the tit-for-tat that this availability demands, the employee may feel that (s)he should be allowed to use the Internet at work to take care of quick business tasks, such as paying bills, sending an email, or checking that evening's movie listings. So long as it isn't excessive, the employee may wonder why the employer even cares. Employers can and do care for many reasons, some more profound than others.

### Goals for Monitoring

Why do companies monitor their employees? Organizations monitor for many reasons, including simply "because they can." An electronic monitoring effort is often difficult to establish and maintain, so before an organization begins such an effort, there should be clear monitoring goals.

The popular press is filled with stories of employees frittering away time on the Internet (Swanson, 2002). In the beginning, employees were likely to spend unauthorized time on the Internet at pornography and gambling sites, but now news and online shopping are more likely outlets for cyberslacking (Reuters, 2002). This is quite the opposite of employers' expectations when they implemented Internet connections.

Responding to these challenges, employers created acceptable use policies (AUPs). Some organizations already had AUPs implemented to keep out electronic games, and they simply modified those policies. Other organizations created new AUPs, which directly addressed the Internet's productivity threat. AUPs are useless without enforcement, but in today's litigious society, it behooves accusers to be certain of transgressions before enforcing the policy. Monitoring tools create an irrefutable log of usage which can stand as legal evidence. Some employers hope the mere threat of punishment will keep employees from cyberslacking, often with some success (Urbaczewski & Jessup, 2002). Below are listed some possible goals of a monitoring effort.

#### Increase Employee Productivity

The Internet was introduced into many organizations as a tool to increase employees' efficiency. While traditional IT packages provided few opportunities for employees seeking to slouch on employer time, the Internet posed an entirely different situation. Computers now had the capability to be an electronic equivalent of a water cooler, break room, or smokers' perch. To curb the potential problem of employees wasting time while appearing to be busy, an organization could implement a monitoring program which completely blocks and/or records the amount of time spent at non-work-related Internet sites. An alternative could be limiting access to frivilous sites to non-production hours only, such as during lunchtime.

#### Bandwidth Preservation

In some organizations, concerns are not productivity-based but rather that network bandwidth is being dominated by applications and instances not directly work-related. An example might be listening to streaming audio

or watching streaming video, both constant drains on bandwidth. People can also engage in excessive file transfers across networks which results in reduced network performance. Two possible solutions to this problem are to purchase more bandwidth or limit the usage of existing bandwidth, with monitoring programs aiding in the latter solution.

### Legal Liability Reduction

Along with productivity and bandwidth usage, organizations are also concerned about Internet usage from the potential exposure it brings to legal liability. Consider the following fictitious scenarios:

*"Organization X today was sued for negligence, as an employee was running a child pornography server inside the corporate network."*

*"ABC Corporation today was sued by a former employee who is now in treatment with Gambler's Anonymous. He is charging that ABC, by placing an unrestricted Internet terminal on his desktop, essentially gave him unfettered access to the virtual casinos thriving on the Internet."*

*"Company B is defending itself today against a privacy lawsuit. It is charged that when an employee downloaded a file-sharing program, that program was equipped with a backdoor which allowed malicious hackers entrance into Company B's networks. These hackers then took thousands of credit card numbers and personal data from the databases..."*

Other possibilities like sexual harassment suits and industrial espionage make the legal risks mount. Organizations indeed may wish to monitor Internet connections to prevent any potential legal liabilities from allowing illegal activities to be conducted on their networks.

## MAIN THRUST

## Different Monitoring Strategies

Once an organization decides it will monitor, it needs to know what to monitor. While Web porn is probably the most reported off-topic use of the Internet in an organization, it is certainly not the only transgression that might come from an Ethernet card. Excessive personal e-mail, filesharing, instant messaging, multimedia streaming, and Usenet browsing and posting are among other ways that employees use the corporate Internet connection for personal enjoyment.

There are several different control mechanisms that an organization might use, generally grouped into one of two categories: managerial and technical. The managerial techniques for monitoring are similar to ways that monitoring of employees has been done for decades: walking around and keeping one's eyes open. When a manager starts to wonder about an employee's performance or collegiality, then the manager starts to pay more attention to that employee's work habits.

Overall, however, the most popular means of monitoring employees is through technology. In many ways, this makes sense – a technical solution to a technological problem. Electronic monitoring operates like "big brother" (Zuboff, 1988), keeping a constant watchful eye on the network and its connected systems (or whatever subset of those systems/hours that a manager may choose to watch). Records can then be kept and offered as later "proof" of an offender's cyberslacking or lack thereof.

## Electronic Monitoring Techniques

### Logging at the Gateway

Many logging technologies are designed to capture and record packets as they enter and leave the organization, or at least the header information that indicates the sender, recipient, and content of the message. Gateway logging is useful in that it provides a central point of network control. However, it is difficult to accurately gauge how long an employee stares at a particular page, and if all that time (s)he is actually staring at that page or if (s)he has actually gone to lunch and returned later. Moreover, gateway logging can be defeated by the use of encryption tools like PGP (www.pgp.com, see McCullagh, 2001, for a more detailed description of an FBI case with the Philadelphia organized crime ring), or even tools like Anonymizer.com that allows a person to surf the Web anonymously using their gateways and encryption tools. In cases where these technologies are used, a separate technology might also be needed.

### Spying at the Client

When gateway logging is insufficient, one can monitor and record connections directly at the source. A keystroke logging program can record everything that a person types on a computer, and many even include technologies to take screenshots or use the Web camera on the desk to prove that it was the person actually sitting at the computer and not someone who just walked up to the terminal.

Client sniffing programs are excellent at recording exactly what the user is doing with the computer at any