Title:
Effective Employee Internet Monitoring

Word Count:
576

Summary:
Many business owners find themselves in the position to confront employees about their Internet use. Non-work related activities including online games, Internet shopping, stock trading, Internet radio, streaming media and MP3 downloads represent the new temptations in the workplace.

Keywords:
network management, internet monitoring, securemycompany

Article Body:
Many business owners find themselves in the position to confront employees about their Internet use. Non-work related activities including online games, Internet shopping, stock trading, Internet radio, streaming media and MP3 downloads represent the new temptations in the workplace.

When an employee connects to the Internet, your company is exposed to these four threats:

- Productivity Threats: Just 20 minutes of recreational surfing a day can cost a company with 30 employees over $1000 per week (At $25/hr per employee)
- Legal Threats: Employees can sue if you don't provide a work environment free of gender and minority harassment. This means taking reasonable care to block offensive Internet content.
- Network Threats: An employee can crash your network just by logging into the wrong website. Other activity like recreational surfing and downloading MP3 files can divert valuable bandwidth from critical business needs.
- Security Threats: Viruses enter networks through a variety of sources, such as web-based email, Instant Messenger file transfer, email attachments or through other files directly downloaded from a website.

Companies of all sizes must effectively incorporate email, Instant Messages and web traffic logs into their overall records management strategy. Some companies must do this to comply with industry regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley and HIPAA.

The first step is to choose the types of Internet content that will not be allowed in the workplace. Keep in mind that not all employees will have the

same privileges, so it is important the network management solution you choose provides a flexible configuration to suit your needs.

There are two basic types of Internet monitoring solutions: Gateway and desktop solutions. Gateway solutions are software or hardware that act as checkpoint for all Internet traffic on the network. Desktop solutions are installed on the local machine to enforce the Internet policies before the request leaves the machine. Desktop solutions work well on smaller networks and gateway solutions work well on both.

The next step is to create an official company policy specifically for Internet use. It should include all Internet activities and not just those you wish to manage. Keep in mind the document cannot account for every possible scenario on the Internet, so it is important to use broad terms with specific examples. For example, instead of stating "Political opinions are not to be posted on newsgroups," you may wish to use "Messages originating from the company network or other company-owned assets may not contain political opinions." The second clause is much stronger because it doesn't specify a message type or delivery system. If you have liability insurance, then be sure to get their approval on all documents. In some cases they will have additional provisions that directly relate to your industry.

The most difficult step will be implementing the new policies. In most cases, some or all users will experience a reduction in Internet privileges. Prepare for a temporary increase in support requests as some users will be prevented from accessing some work-related content. Internet policy configuration is an on-going process that must be routinely maintained.

Soon the complaints from users will cease and production will return back to normal. It is important to keep your filtering software updated and to maintain a history of Internet activity. If the time comes when you must confront an employee about their Internet use, you will have proof of their Internet activity and a detailed comparison to their peers. That is a much stronger case than saying "I've seen you 10 times looking at …."