

GFI WHITE PAPER

INTERNET MONITORING: NOT 'BIG BROTHER' BUT 'WISE MANAGEMENT'

Internet usage is now ubiquitous in every modern business. When employed properly it can be an extremely efficient and highly effective productivity enhancer. With the Internet, employees can keep tabs on critical changes, perform research and any number of business tasks. Email, another aspect of the Internet, allows for near instantaneous communication of business data. If either is unavailable, even for short periods of time, you can almost hear the grinding of gears as the entire enterprise comes to a halt. System failure is not the only potential problem however, unscrupulous or apathetic employees who choose to forget what the Internet and email are there for, can be just as damaging.



Internet Monitoring: not 'Big Brother' but 'Wise Management'

Internet Misuse

In an ideal world everything conducted at a business would be related to a business, but that isn't always the case. Just as the telephone, company car, and photocopier have been used for non-business related matters, so too has the Internet and email. Consider the following statistics:

- According to IDC Research, 30% to 40% of Internet use in the workplace is not related to business.
- In a survey conducted by Sex Tracker, 70% of all Internet porn traffic occurs during the normal workday of 9-5.
- A study by Vault.com revealed that 37% of workers say they surf the Web constantly at work on personal rather than business matters.
- The cost of employees surfing the Web from their office PCs is estimated to cost US companies more than \$1 billion dollars a year (<http://surveilstar.com/employee-internet-monitoring-research-resources.html>).

In addition, companies are now facing challenges from Internet misuse that include:

- Time and productivity losses by employees using company time to visit non-business sites
- Bandwidth limitations when personal Internet use clogs up network access
- Security threats when hackers or harmful applets enter the corporate network from unsecured websites
- Legal repercussions when objectionable or dangerous material is introduced into the business environment.

As can be plainly seen, the net effect of inappropriate Internet usage can damage an enterprise's productivity by reducing revenue, increasing costs and exposing the business to unwarranted litigation. In its simplest terms, abuse of Internet access can be a significant cost factor to doing business.

Internet Monitoring

There is an increasingly larger number of businesses that monitor what their employees do on the Internet in the workplace, with studies revealing that about half of all corporations routinely use various methods from email monitoring and website blocking to phone tapping and GPS tracking, combined with policy to manage productivity and minimize litigation, security, and other risks.

Employers are primarily concerned about inappropriate web surfing, with 66% monitoring Internet connections. A total of 65% of companies use software to block connections to inappropriate websites, especially sites with sexual, romantic, or pornographic content; games; social networking; entertainment; shopping or auction and sports. Others use URL blocks to stop employees from visiting external blogs.

Whether or not employers should engage in this practice or not often leads to a serious and spirited debate that puts an individual's right to privacy vs. the organization's right to security at the center of the controversy. So far, the courts have upheld the right of a business to conduct surveillance and monitoring of what happens in the workplace, and there isn't any indication that this will change.



Internet Monitoring: not 'Big Brother' but 'Wise Management'

Businesses have been aggressive in protecting themselves and their corporate resources. To date 28% of employers have fired workers for misusing email and nearly one third have fired employees for misusing the Internet, according to the 2007 Electronic Monitoring & Surveillance Survey from American Management Association (AMA) and The ePolicy Institute.

Pros and Cons

Before a business makes the decision to monitor their employees' Internet habits and how they spend their time online, there are some definitive advantages and disadvantages to consider.

For a business the principal advantages are the obvious need to protect the enterprise's assets, including equipment, networks and data. These items are all pivotal to business operations and if any are damaged or lost, the company could incur some serious damage and/or legal consequences. Other key advantages to employee Internet monitoring include:

Confirm that Internet use is not Internet abuse

While most employees are likely to not abuse their Internet privileges at work to the extent of abuse, unfortunately the reality of it is there is a percentage that usually will. As we have already explained, employees that abuse the Internet for purposes other than work lower the business's productivity level because if they are busy hanging out on social networking sites, such as Facebook, or surfing the web, they are not doing the job they were hired to do. And that not only costs businesses, but is also a form of fraud.

Monitoring allows for identifying the culprits and dealing with them, rather than being forced to take a global action, including barring all access or introducing draconian measures that may be necessitated by the actions of a few.

Another problem associated with inappropriate Internet use is when employees use their work e-mail address for mailing lists or other personal reasons. Usually when employees use their work e-mail, the end result is spam which is costly for the company.

Increased Security and Better Risk Management

If a company's network or workstations are infected by any kind of malware, this could either interfere or halt a business's daily operations. Any kind of infection that attacks computers on the employer's network can pose serious consequences for the organization; sales could be lost, orders may not get processed in time, or the supply chain could get interrupted. Additionally, depending on the kind of infection, data could be compromised or stolen which could lead to legal repercussions and risks for people whose personal information was stored in the databases.

Monitoring employees' Internet use also means it is less likely they are going to be involved in activities that can expose the company to litigation ranging from sexual harassment to out and out fraud.

The cost of fixing any problems can be high, and monitoring is a far less expensive alternative to dealing with a data breach, extensive periods of down time or lawsuits.



Improved Productivity

Employees who are aware they are being watched are likely to spend more time working and considerably less time on personal matters. This translates to an increase in productivity and considerable cost savings by increasing a company's return on investment.

Organizational and Personal Accountability

Internet monitoring makes it clear to employees that certain behaviors and norms are expected in the workplace as part of the corporate culture. Some companies have written policies about Internet usage in terms of which sites employees should not be visiting during company time (see GFI's White Paper on [Internet Acceptable Use Policies](#)). Without a monitoring system in place, some employees may feel like they can do whatever they want. On the other hand if employees feel like they are being monitored, they may not go to certain sites in the first place.

Disadvantages

Despite these obvious advantages to Internet monitoring, there are some disadvantages that need to be considered.

Employees may resent being monitored. Feeling they are not trusted is a sure way to lower morale. Studies have shown that lower moral inevitably leads to reduced productivity.

Another disadvantage is final. Internet monitoring costs money and a company will need to hire, either as employees or contractors, people to review the information. In a large company engaged in proprietary activities or whose operations are politically sensitive, such as a large oil company, this may be feasible. For a small business with only a few employees, the return on investment may be low or non-existent.

Another, though not very obvious, disadvantage of workplace Internet monitoring is what to do with the information once it has been collected. People do strange things, some of which may lead your organization into unexpected places. While you can readily determine that pornography has no place in the business environment, what about the rest you may uncover? If a person is frequently visiting a site associated with criminal activity, do you call the authorities? If a married staff member is frequently visiting dating forums, do you tell their spouse? What if someone was on a personal site for three minutes during lunch? What do you do when you find out your top employees are on Facebook for at least three hours every day? There are a hundreds of other scenarios to consider, but too much information may be more of a burden than a benefit, and open the company up to additional risk.

Despite these disadvantages, sometimes Internet monitoring is a necessity in the workplace and security, productivity and proper use are three strong reasons to monitor because of the many advantages associated with these reasons. Therefore the best approach is for a company to view Internet monitoring from a business perspective and explain the reasons for Internet monitoring to the employees from that perspective, thus making it less personal and more work-oriented. In those circumstances, employees are more apt to accept the monitoring as a necessary evil, rather than an attempt by management to create a Big Brother environment.



Ethical Monitoring

If as a business, you decide your company should be monitoring, it needs to be employed in an ethical manner. In other words, Internet monitoring should follow some basic rules that assure its proper application, in the correct manner, for the correct reasons.

Acceptable Use Policy

The first step in any ethical monitoring system is to develop a Computer and Internet Acceptable Use Policy that all employees are required to read and sign. The policy should make it clear that employees should have no expectation of privacy while using business related computing assets. In conjunction with Human Resources, the document should clearly identify what is expected of employees and what activities will not be tolerated, as well as explaining the consequences of any violations. This places everyone "on the same page" when it comes to computer, email and Internet use at work. It also means that any necessary disciplinary actions can be taken without hindrance since prior notice has been given.

Ethical and Unethical Uses of Internet Monitoring

Courts have consistently supported Internet monitoring and actions based on it by companies against misbehaving employees as long as the monitoring has been for legitimate business reasons. The key measures of what has been legitimate have been:

- Cost reduction
- Safeguarding company information
- Maintaining a professional and comfortable workplace
- Upholding a company's ethical values
- Reduce liability.

On the other hand, Internet monitoring, done for the following reasons, is considered unethical and typically rejected as reason for monitoring, and hence any subsequent actions:

- Targeting a specific employee solely for the purpose of termination
- Viewing personal data of the employee not relevant to work
- Application of personal, rather than business, moral and ethical standards
- Personal gain.

Conclusion

Internet monitoring in the workplace is an important consideration for any enterprise. If circumstances warrant it, then a business has an obligation to take the steps necessary to protect itself from the actions of employees who act in a fraudulent manner by misusing and abusing the Internet while at work. If a company decides to employ Internet monitoring in its environment then it must do so by providing prior notice to its employees. Monitoring must be for legitimate business reasons and conducted ethically.



Internet Monitoring: not 'Big Brother' but 'Wise Management'

How GFI WebMonitor™ can help an organization

GFI WebMonitor, an award-winning solution currently being used by thousands of customers, gives organizations comprehensive control of the use of the Internet by employees in the workplace, performing both Internet monitoring and web security. It gives management the ability to monitor Internet browsing, block access to sites on an individual or group level, provide protection against hidden downloads as well as block and identify background processes that are downloading payloads which may be malicious in nature or use up network resources.

GFI WebMonitor allows administrators to manage what sites users can browse and block access to websites in particular categories, such as adult material, online gaming, personal email, Peer-2-Peer, Facebook, MySpace, and more. Web monitoring is made easy with an extensive database that provides URL coverage and categorization for 205,000,000 domains and that is being continuously updated.

GFI WebMonitor also offers web security features that allow you to monitor what files employees are downloading, to block file-types such as MP3s and movies and to scan all files for viruses, spyware and malware using multiple antivirus engines. GFI WebMonitor lowers the risk of phishing by blocking access to phishing websites through the use of an auto-updatable database of phishing URLs. The web monitoring features also allow you to monitor and block Windows Live Messenger (MSN) chat sessions and file transfers.

It is also available as a dedicated plug-in for Microsoft ISA/TMG Server.

For information on GFI WebMonitor visit <http://www.gfi.com/webmonitor/>.

© 2010. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.