

GFI White Paper

Why SMEs need to deploy a web monitoring tool

Most organizations today use the Internet to conduct business, giving employees access to what is, without doubt, an essential business tool. However, non-work related Internet use by employees is a common and growing concern for management. One effective way of maintaining comprehensive control is to use a web monitoring and web security solution.

This white paper explains why.

Contents

Introduction.....	3
“Time is money”.....	3
Is this a problem for your business?.....	4
Other problems.....	4
What to do?.....	4
Ethical and unethical uses of Internet monitoring.....	6
Summary.....	6
About GFI®.....	6

Introduction

You are going about your workday as the head of a small or medium-sized business (SME) sitting in your office when there is a knock on your door. Your assistant shows in a visibly upset customer who clearly wants to talk to you. In a few minutes she sketches out the cause of her irritation. She arrived at your business and sat for 20 minutes waiting for service while one of your employees was busy on the front office computer.

"After 15 minutes had gone by," she says, "I stood up to ask the clerk how much longer it would be. I could see the computer screen reflected in the glass of the cabinet behind her. She was in the middle of playing a computer game! What sort of business are you running here?"

The above story is repeated far too often to the dismay of businesses, large and small. The clerk was engaged in cyber-slacking – wasting time online instead of working and it is only one of the many problems faced by today's businesses from unlimited and uncontrolled access to the Internet.

Never before have employees been so eager to go to work and focus attention on their computer screens. But what passes for enthusiasm for work is often enthusiasm for using the employer's computer system, at an enormous cost.

Instant messaging, always on, carries messages from others who are also wasting time at work. Communications that never would have been made during the workday, given the ease and instantaneous gratification of a reply, are made all day long.

The sites that eat up productivity at work include eBay (you name it, you can find it on eBay), travel sites (where employees can plan their vacations, usually at a discount), E-commerce sites over the holidays, social networking sites, car-shopping and price-comparison sites, pornography, fantasy sports, horoscopes, banking, investment and stock-watch sites, cyber-dating services, and, to rub salt in the employer's wound, job-hunting sites. Some of the newest rages online catch on first in the workplace. It's a matter of faster access and fewer interruptions than at home. And where downloading full-length movies and lots of music files are concerned, endless storage capacity on the network's servers!

"Time is money"

Every minute spent cyber-slacking increases costs and reduces profits. Workplace productivity is the number one underlying reason for loss of profits within a company.

Employees using the Internet during the workday to conduct such personal tasks as stock trading, online shopping, online auctioning, online games, personal emails and chats, downloading software and music and so on, are a productivity leak.

According to a recent Gallup Poll, employees spend roughly 75 minutes each doing the activities mentioned above. Using the US average salary of \$20 per hour, this results in an annual loss of \$6,250 per employee. Table 1 shows the cumulative cost of this activity, assuming a work year of 250 days:

# of employees	salary / hour	loss / year
1	\$20	\$6,250
1	\$50	\$15,625
10	\$20	\$62,500
10	\$50	\$156,250
50	\$20	\$312,500
50	\$50	\$781,250
100	\$20	\$625,000
100	\$50	\$1,562,500
500	\$20	\$3,125,000
500	\$50	\$7,812,500

Table 1: Estimated dollars lost to cyberslacking

In other words, if you are a company with 500 employees and you pay them \$20 per hour you could be losing as much as \$3 million dollars every year in lost productivity.

Is this a problem for your business?

Consider the following data:

92% of online stock trading occurs from the workplace during work hours.

30% of American workers watch sports online while at work.

24% of American workers admit to shopping online while at work.

According to Nielsen Ratings, employees use company's high-speed Internet access to visit sites such as Broadcast.com and MP3.com more frequently at work than they do at home because of the high-speed Internet access at work.

IDC Research found that 30 to 40% of Internet use in the workplace is not related to business.

70% of all Internet porn traffic occurs during the nine-to-five work day according to 'sex tracker'.

In a 2009 Valut.com study 37% of workers admitted they surf the Web constantly at work.

The odds are that you already have suspicions about a few or many employees abusing their Internet privileges throughout the work day. These are the ones who cannot complete their work on time even while given adequate time to do so. These are the ones who close windows as you or someone else walks by.

Other problems

In addition to lost productivity, SMEs, like large businesses have to be concerned with a host of other Internet related threats that can affect their bottom line, and even the very business itself.

These include:

Introduction of malware

With the number of web threats growing and the increased sophistication of cybercriminals, all it takes is for an employee to visit or download a single piece of malware to compromise your business in any number of ways. For more information on web-based threats, see the GFI White Paper: '[Web based threats](#)'.

Leakage, intentional or not, of confidential information

One of the most important assets in your company is the information you withhold. This can be trade secrets, source code and programming, records, customer information and contacts, strategies, product development and much more. All of the above are readily available to your employees and thus are subject to being leaked out of your company to the wrong hands - possibly competitors.

Bandwidth usage

Bandwidth costs money. Employees spending time browsing non-work related sites with streaming content, playing online games or downloading large files have an impact on network performance and use up bandwidth that is required for essential or critical services. Exceeding contractual bandwidth limits or purchasing additional bandwidth can cost businesses a considerable sum of money and an unnecessary expense.

What to do?

There are basically two options to addressing the problems outlined so far. The first and most extreme, is to cut off access to the Internet entirely. This may work effectively for some employees who do not need it; it is sometimes necessary to cut off Internet access altogether for employees such as bank tellers, floor nurses or security staff, who don't need online access as part of their job.

While this may be effective for a portion of your workforce, it is unlikely that you will be able to apply it to every single employee – using the Internet at the workplace has become an integral part of doing business in today's information age. And most experts believe that cutting off Internet access is throwing the baby out

with the virtual bathwater. Along with the wasted time comes improved productivity when the Internet is used as intended. Many studies have been conducted in which employees have indicated that they would sooner give up the phone than email at work.

An increasingly larger number of businesses now opt for a second option and deploy software that prevents access to inappropriate sites, filters keywords and monitors against malware, thus allowing continued Internet access by employees who need it, while at the same time protecting the company's assets.

Studies show that employers are primarily concerned about inappropriate web surfing, with 66% of them monitoring Internet connections. 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.

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.

For a business, the principal advantages to web monitoring is how it can be used to protect a company's assets; including equipment, networks and data. Other key advantages to employee Internet monitoring include:

Confirm that Internet use is not Internet abuse

While most employees are likely to not use their Internet privileges at work to the extent of abuse, there is a percentage that will. As already explained, employees that abuse the Internet for purposes other than work related lower the business' productivity level because if they are busy hanging out on Facebook or surfing the web, they aren't doing the job they were hired to do. That not only costs businesses, but is a form of fraud.

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

Increase security and optimize risk management

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.

Maximize productivity

Employees who are aware they are being monitored 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.

Establish 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 know they are being monitored they may not go to certain sites in the first place.

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 is legitimate are:

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

Summary

Sufficient evidence exists that Internet misuse is a widespread problem in every company that has an Internet connection. Misuse borders from the occasional transgression to serious impact of a company's productivity. Cyber criminals have and will continue to exploit vulnerabilities wherever they find. Being without a basic protection methodology such as web monitoring is a shortcut to financial ruin.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at <http://www.gfi.com>.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com



Disclaimer

© 2011. 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.