Global Information Assurance Certification Paper

Why The Need for Internet Content Filtering/Management- A Close Look at Internet Manager Elron Web Inspector 6.03

by Michell R. Singleton
GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b, option 1

Abstract

In the last ten years, the Internet has changed the way companies do business. From companies that need real time information, to companies having business applications on the Internet, the Internet has become essentially a required tool. With the requirement of this tool, a lot of issues stem from employee surfing, such as lost productivity, Internet abuse and legal issues.

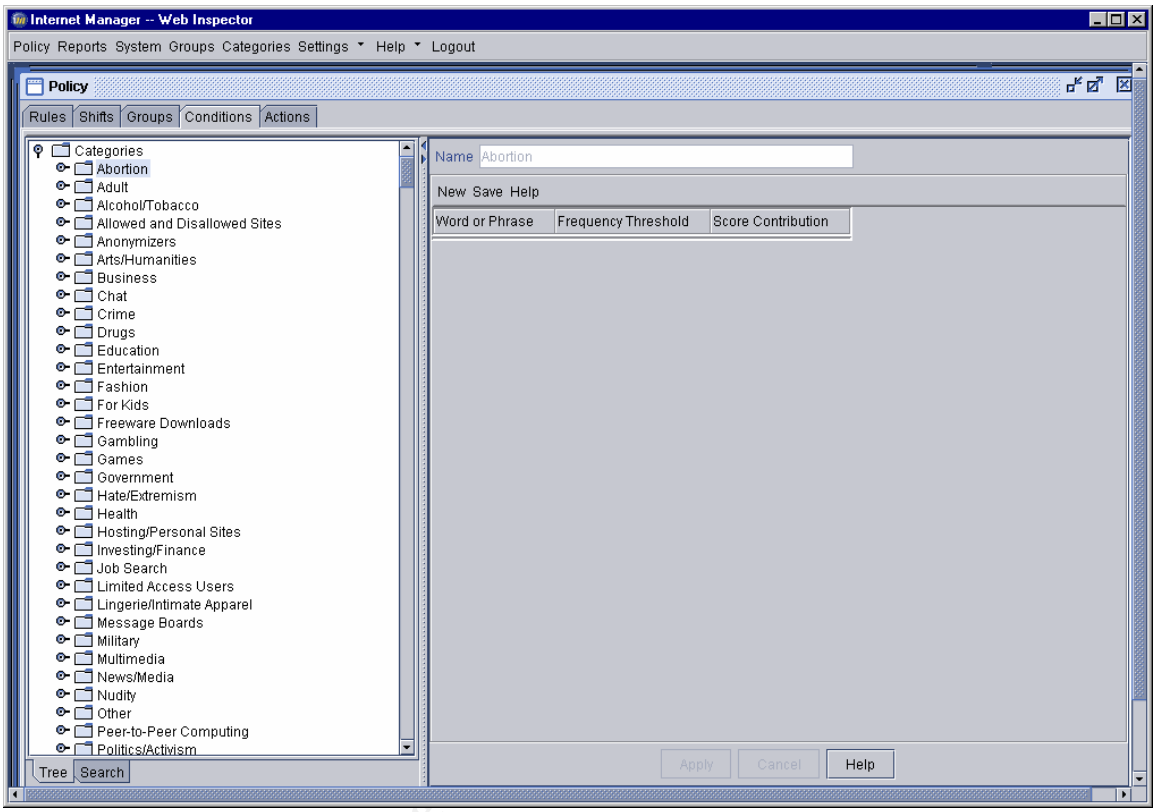
Today, there are a lot of software products designed to help reduce Internet abuse, help employees abide by the company's Internet usage policy, sometimes called an acceptable use policy. This, in turn, helps companies protect their intellectual property and public image. I will examine one of the top software products for web content filtering, a software product called Internet Manager Web Inspector 6.03 from Elron. I will also examine how it works (SmartList™ technology), briefly discuss how to install and setup and what impact or savings it can provide for a company. I have limited my discussion to the Windows NT/2000 platform only and have not discussed any other operating system platforms such as Netware, Mac, or Unix. This paper will assume the reader knows about and has in place an Internet usage policy. The intent and conclusion of this paper is to show the reader the need or value of web content filtering and discuss some installation aspects and/or setup and features of the Elron software.

Features of Elron Internet Manager Web Inspector 6.03

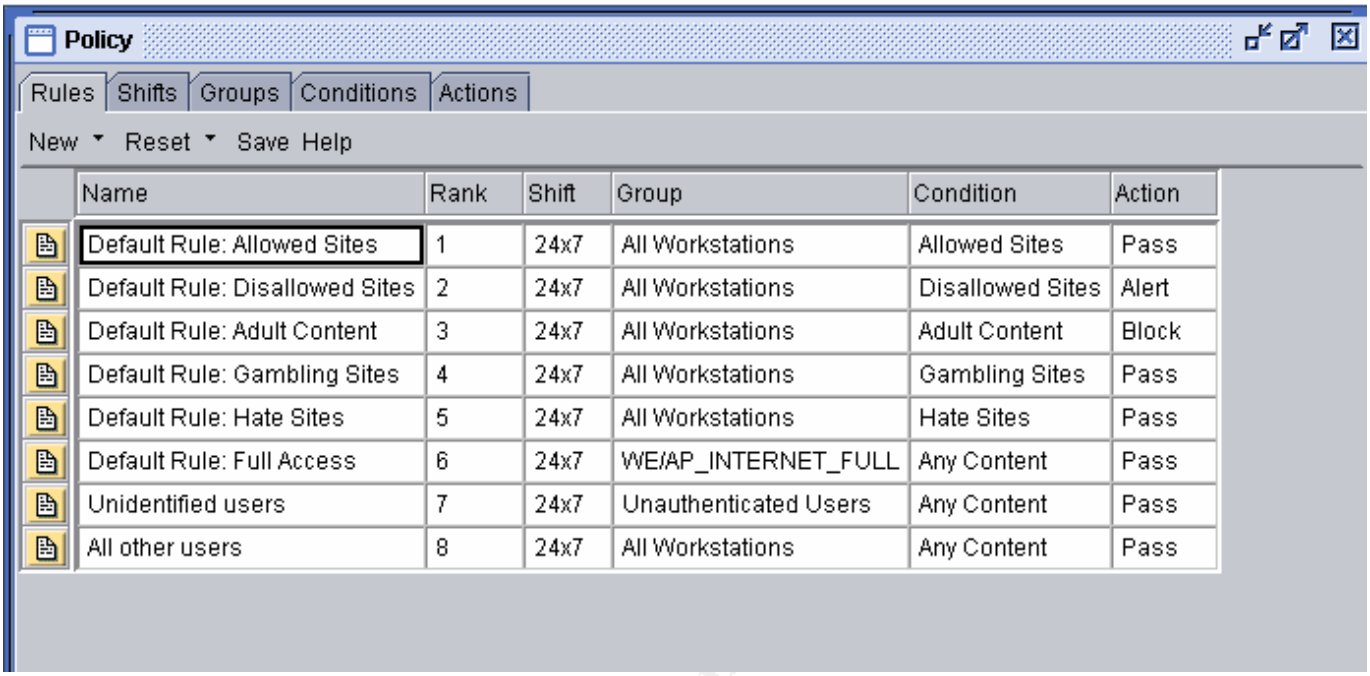
Elron Web Inspector uses a SmartList™ technology to scan the actual content of the web page, in addition to the URL name (9). Elron Software's proprietary Smart List dynamic approach to Internet filtering, rather than the subscription-based block list, provides for an easier way to receive updates than to shutdown your system to receive updates. The Web Inspector product categorizes each web site that it scans using a SmartList™ technology. Web Inspector comes with default categories and sites in them. The sites can belong to any number of categories and you can customize each site to be added/removed from a category. If a site doesn't match any of the default categories, then Web Inspector will place the site in an "Other" category. When Web Inspector scans a page that it doesn't recognize, it will examine the content of that page and the

root of that page for any matches to any categories for which the SmartList™ category and dictionary has defined. With Web Inspector, you can decide the types of content you want to monitor by customizing the SmartList™ dictionary.

An example of the default category and site are shown below:



With Web Inspector, you can create a policy that will be able to block all web sites that violate your Internet usage policy or a category (sexually explicit, adult, etc.), that you feel employees should not have access to (1). The policy can setup various rules to allow a certain group or individual access or block them; can impose conditions to allow/deny a category access or not; could create an action (pass, alert or block) necessary if a rule in the policy was violated. The alert condition could send an automated email immediately to you, so that corrective action, further evaluation, diagnosis or investigation of a potential problem could take place right away. With this dynamic feature, you will always be ahead with a potential liability and could address it immediately. Web Inspector is very flexible as you can customize the policy to your needs. An example of a policy is shown below.



Name	Rank	Shift	Group	Condition	Action
Default Rule: Allowed Sites	1	24x7	All Workstations	Allowed Sites	Pass
Default Rule: Disallowed Sites	2	24x7	All Workstations	Disallowed Sites	Alert
Default Rule: Adult Content	3	24x7	All Workstations	Adult Content	Block
Default Rule: Gambling Sites	4	24x7	All Workstations	Gambling Sites	Pass
Default Rule: Hate Sites	5	24x7	All Workstations	Hate Sites	Pass
Default Rule: Full Access	6	24x7	WEAP_INTERNET_FULL	Any Content	Pass
Unidentified users	7	24x7	Unauthenticated Users	Any Content	Pass
All other users	8	24x7	All Workstations	Any Content	Pass

Web Inspector monitors all web traffic that passes it by default by the workstation names but you can configure the system to track by username by implementing user authentication. When Web Inspector collects data using a promiscuous port on the network, it uses Transparent User Authentication (TUA) functions to associate a workstation name and user name with each HTTP request. Once implemented, it will automatically add usernames to the database or any new usernames that may login to the machine, thereby minimizing the user management work for security administrators. This authentication is nice because the users do not need a separate login for web access and it is invisible to the users when installed. The TUA is great because it doesn't utilize a lot of resources as a communication mechanism with a small, keep alive, user datagram protocol (UDP) packet. Keep in mind that the TUA is necessary for accountability if you have users that can roam among several workstations, users share a workstation or it is just too difficult to decipher a user from a workstation.

Web Inspector has several ways to import data. It could be done either manually through the Web Inspector Console, from a file using either the Web Inspector Console or using Web Inspector's utility user interface called WI Utilities. You can also import data from the NT domain or directory using WI Utilities or by using a command line utility. This methodology Web Inspector has of importing data can add users, workstations or groups.

Importing Data Manually

In order to add users, groups or workstations manually, you will need to go to the Groups page right click and select either All Users-Add User, Groups-Add Group or All Workstations-Add Workstation in the Web Inspector Administrative Console.

Importing From a File Using the WI Console

Using an text editor such as Notepad, type the data needed in the Web Inspector format shown below and then save the file in a .csv or .tsv extension, depending on if you decide to use commas or tabs to delimit the data:

Standard User Format: Email Address, Full name, Last Login

Email@address.com	Full Name	“”

System User Format: Email Address, Full name, Last Login, Username, Password

Email@address.com	Full Name	Username	Password if a system user

Once you have completed entering all the data, save the file. On the Groups Page right click All Users-Import, select the file, click Open.

Importing From a File Using WI Utilities

In order to import from a File, select Workstation or User Group Import then file. Importing from this file must have the following format below shown as a .dat extension:

Workstation Standard Format

[Workstation Group S]
Workstation, IP Address, Licensed, Authenticate, Domain

User Standard Format

[User Group S]
Username, Full Name, Email Address, Email@emaildomain.com,
Usernameb,, Email Addressb, Emailb@emaildomain.com,
Usernamec,Full Name,,Domain

Importing Data from an NT Domain or LIGHTWEIGHT DIRECTORY ACCESS PROTOCAL (LDAP) directory Using WI Utilities

In order to import from an LDAP directory such as Microsoft Active Directory Service (ADS) select User Group Import then LDAP. Next, you will need to add the server's IP address or Fully Qualified Domain Name (FQDN) in the server box. Next, enter the container where the search will begin in Node. Select Query, then pick the available groups. Shift the available groups to the group import list. Before selecting import, MAKE SURE that your Configure button is customized to how you desire.

In order to import from an NT Domain, you must first verify the Web Inspector is running Windows NT Server, Windows NT Workstation with NT Server tools or Windows 2000 and that you are logged on as administrator. Then select User Group Import-NT Domains. Next, select the available groups then shift the available groups to the group import list. Before selecting import, MAKE SURE that your Configure button is customized to how you desire.

Importing with a Command Line Utility

You can run WI Utilities from a command line window, in order to import user groups from a text file, an NT 4.0 Domain, or an LDAP Directory. The user group application has five modes (-b,-c,-f, -n,-p) to help achieve this. The following table will show the modes and their description:

-b	Import from LDAP directory with specified domain name and node name
-c	Import from LDAP directories with a specific file that contains a list of domains
-f	Import from file that contains user groups
-n	Import from a specified Windows NT Domain
-p	Import from a network with a specified file that contains a list of Windows NT domains

Now whether you import LDAP or Workstation or User Groups, you must have a correctly configured file called WiLDAPattrs.cfg, UserGroupImport.cfg or WksGroupImport.cfg and must be saved in the same directory as WI Utilities. Once you open a command window, just type any one of the files with a .cfg [-b,-c,-f,-n.-p] [domain].

Web Inspector's real-time reporting and web-based interface gives you the ability to view simple, but detailed reports on Internet usage (10). The reporting feature provides for a way to access the data immediately. This data can view the amount of surfing in minutes by day or hour. If you wanted to see what sites are

being accessed, you could do so. If you suspect an employee may be abusing the Internet, you can use Web Inspector to ensure that you have the right individual. Web Inspector provides over 500 different types of reports that you can customize if you desire (12). Depending on how you have the software setup, reporting can be done by user id, workstation name or IP address. The Web Inspector is also web-based, so you can easily administer the product from a remote location. Web Inspector can provide real time monitoring of various sites and you customize and create various reports based on surftime or accesses by employee, workstations, user groups, site or category reports.

Web Inspector has also a reporting feature that can estimate how much internet surfing costs in your company given in work hours, based on an average salary and the time spent surfing since Web Inspector was installed (8). This cost option is located in the surftime reporting. Web Inspector has a default cost setting of 24 cents per minute/$30,000 annual salary but you can customize that setting to your company's typical employee salary.

Web Inspector has features that may be important when creating reports. Web Inspector has some default groups that you may not want monitored or restricted. The groups are called Unrestricted Users and Workstations. These typically may be your security administrators that need to be added to these groups so they can bypass the Web Inspector policy and complete investigations to potential block sites. Also you can add sites to a group called unmonitored sites.
In doing this, you will be able to block all ad websites from being generated within your reports. This is an excellent feature because then the report is not cluttered with all the pop ups that various websites have.

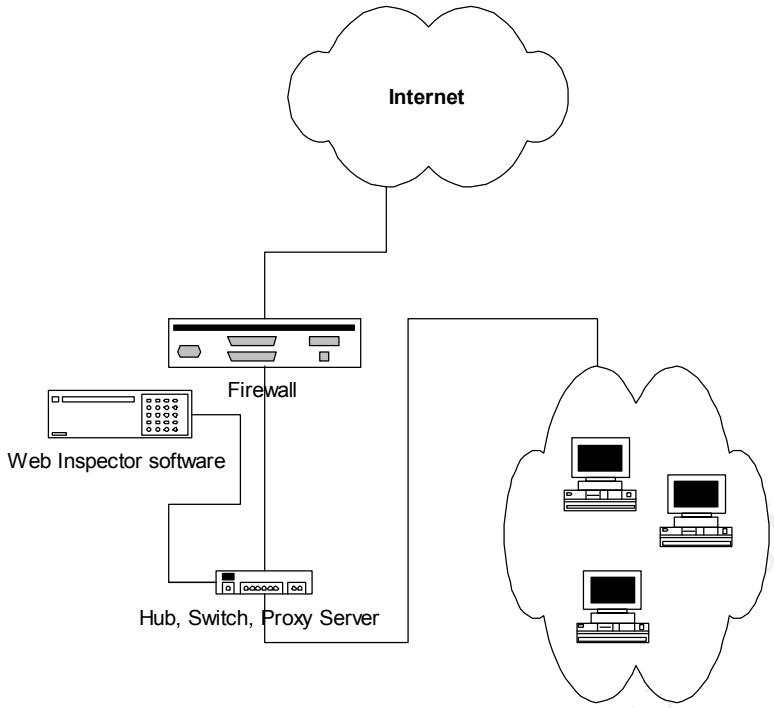
Web Inspector plays a huge role in its ease of use with archiving data. In my area of responsibility as a security administrator, there exists a need to view the historical data for security investigations. Whether the data is for an investigation of a breach of a potential security issue or analyzing a surfing pattern of a user or group, anyone without a SQL or MSDE database background can do this easily. Web Inspector provides detailed, simple instructions using a command file and how to automate the process through an AT batch command scheduler program. Keep in mind, that it would be a better idea to have a second server as an archived server so that when you won't disrupt current data collection in order to view prior months activity.

Installation and Setup of Elron Internet Manager Web Inspector 6.03

Installation is quick and can be setup in minutes. It is very important that you pick the correct location in your network, so Web Inspector can scan all traffic that passes through it. Next, pick a database (either MSDE or SQL Server) technology engine supported by the product, then install. A typical sample

network placement drawing of Web Inspector is shown below but read the install directions carefully so that you will not reduce Web Inspector's effectiveness at controlling Web access (1). If your network has a setup using a Firewall to *Proxy Server* to network (workstations), then placement of Web Inspector can be tricky depending on how you have your network configuration. For example, if you have a One-Nic Proxy, where the setup is Firewall to Hub to Switch to network, with the Proxy off the Hub, placing Web Inspector on that segment will ensure that it will see all the traffic that passes through it. If you have a network configuration where you have a Two-Nic Proxy, such as the Firewall acting as a proxy, then Web Inspector can monitor the traffic if the following: Communication between browsers and proxy are based on HTTP proxy protocol (Not Socks, Winsock, or another proxy protocol) or placement of Web Inspector is on the inbound side of the proxy server so it will receive all the traffic flowing to the proxy. If your network has a setup using a Firewall to *Switch* to network, then place Web Inspector on the mirroring point of a switch. Please remember the mirroring port must mirror traffic going to the firewall and must be bi-directional, then Web Inspector can see all of the IP traffic for the workstations leaving and entering the network. If your switch doesn't support mirroring, then you can use an unmanaged hub and connect Web Inspector to the hub and then the hub to the switch, therefore making the setup become Firewall to Hub to Switch to network. Web Inspector has a plug-in for MS Proxy Server 2.0. So if you have the configuration of Firewall to Switch to Network, where MS Proxy Server 2.0 is off the switch segment, you can install Web Inspector directly on the host that runs MS Proxy Server.

Also keep in mind minimum browser and hardware setup requirements. If you don't have minimum hardware requirements, Web Inspector may run slow or not at all. As a rule of thumb, always look at your company's network environment to determine the best system requirements. You should also check your browser version, there is a minimum version Web Inspector needs (Internet Explorer 5.5 or Netscape 6.0 or later) or your reporting and remote interface will not work. The administrative console for Web Inspector is a Java based, virtual machine application that allows for local or remote administration.



Once setup is complete, use the administrative console to configure the IP address ranges you would like Web Inspector to scan. After the IP address ranges are configured, Web Inspector automatically starts scanning by the workstation name. Also use the administrative console to setup user groups and the system configuration and policy to meet your companies needs.

If you have a network where users can logon, to multiple workstations, then you would want to implement the TUA. By implementing TUA, you will be able to know which user is accessing the machine, than by just workstation name. The TUA will track user logon with a UDP login, keep-alive, and logout message sent periodically to the Web Inspector server from a workstation running Windows NT/2000. The TUA is then enabled by an authentication method you choose whether you use the user authentication module (UAM) or lightweight user authentication (LUA) module Internet Manager Web Inspector (3). Both modules achieve the same result by providing TUA, but the installation of one versus the other may be better for your company. The UAM module is a self-extracting executable file, that must run each workstation for the first time. The LUA is also an executable that runs but it exists on a file server and can be executed through the login script.

Why Internet Content Filtering/Management is Necessary

Some reasons and examples of why the need to monitor Internet usage are listed as follows:

- Protection against any legal liability or computer crime issues

- Helps promote employee productivity and efficiency
- Enforces the internet usage policy
- Ease of security investigations of improper use of the internet
- Reduces network congestion
- Protection of company intellectual property

A good, clear Internet usage policy should detail what information may pass or not pass via the Internet along with some type of software to backup the policy (4).

On the average, workers spend 21 hours per week online at the office (13). The U.S. Treasury Department recently monitored the Internal Revenue Service (IRS) workforce's Internet use (13). They found that activities such as online chats, shopping and checking personal finances and stocks accounted for 51 percent of employees' time spent online. A large company, 20th Century Fox perceived this as a potential problem and wanted to combat it right away. 20th Century Fox also knew that the unnecessary surfing could be up to the six major categories are pornography, gambling, illegal activities, hate sites, tasteless material and violent content (6). They wanted to enforce their Internet usage policy. Web Inspector provided a vehicle to do that, thereby identifying workplace Internet abuse (2). JFK Medical Center also wanted to assess the Internet usage of their employees and installed Web Inspector. JFK was shocked to find out how much surfing was the sexually explicit, pornographic type websites (11).

As broadband continues to become increasingly popular, companies are becoming bottlenecked. Streaming media, MP3 music files, video and audio files, large graphic files, bandwidth intensive applications that use the internet and simply spending a lot of time surfing all result in slower networks and increased network crashes. A recent study of workplace computers indicated that music swapping software was found on about 20% of over 15,000 work PCs examined (13). In fact, Web users at the office take advantage of high-speed connections to access broadband entertainment sites and MP3 more frequently than at home (13). An estimated 67 percent of IT managers are facing bandwidth increases (13). For many companies, network quality may be their most important business asset (13). If the network is slow, so may be the company's ability to keep pace with competition (13). Today's Internet lets employees buy products, chat with friends, visit their kids at daycare, listen to real-audio feeds and MP3s, and play interactive games. As a result, bandwidth suffers. If those companies would implement Internet Manager Web Inspector, the network congestion would dramatically decrease.

20th Century Fox realized where the network problems lie when they install Web Inspector. Remember, with Web Inspector you can create various reports that will show you specific Internet usage traffic by the top users whether by surftime

or number of accesses (often called hits). The surftime reporting can show the top users and their amount of surfing a workstation and you can create a more detailed report to show exactly what site the user is surfing. With 20th Century Fox viewing the various reports, Web Inspector showed 20th Century Fox that an application server was using 60% of the network bandwidth. Because the Internet reports showed this workstation with the most usage, they were able to redirect that application's Internet traffic to a dedicated server. If they hadn't installed Web Inspector and analyzed their Internet usage reports, the network bottleneck would have cost $15, 000 to $20, 000 dollars more per month as a major network upgrade (2).

More and more companies are faced with a potential legal issue or adverse publicity as employees are spending more time surfing the Internet than working. Over the last couple of years, lawsuits have increase just due to an employee being offended by what they saw on a fellow co-worker's computer screen. The following are good examples where content filtering/monitoring for inappropriate use was needed to protect the company's image and public perception: The highly publicized case of the Patrick Naughton, Infoseek executive, head of the Walt Disney Company Web sites was arrested and charged with using the internet to solicit sex with a minor (5). Also examine the pending case of the San Francisco police officer Michael Block that was suspended pending an investigation of his downloading pornography from the Internet on his computer (7). If the companies had setup a web filtering policy to block all sexually explicit, chat and/or adult sites, the company image may not have been tarnished or in the headlines.

As a security administrator blocking pornographic, sexually explicit sites is key. In doing this, it will help enforce the Internet usage policy.
Typically, you would want to setup the blocking of Web Inspector to the following categories: sexually explicit, hate/extremism, nudity, chat sites, gambling and adult sites. These categories are considered websites that have in the past and may still produce potential lawsuits to companies. This blocking effort will help increase employee productivity and make them more efficient since they know it is not available. Another way to encourage users to adhere to the Internet usage policy is to generate reports for the above categories. The reports that are generated could be sent to the user and/or supervisor. Oftentimes just to see the evidence on paper may help to encourage employees to abide by the internet usage policy and help reduce costs with the unnecessary surfing.

In my security area, Web Inspector plays an important part of security investigations. If there is a breach of security or potential theft using the Internet with a company computer, Web Inspector can help find the information. Because of the ability to archive the data and the fact that Web Inspector scans every site that it sees, security administrators can look at older data to investigate a

possible problem. Without this archived data, companies would not have the proof needed to protect the company against potential lawsuits.

Clearly, content filtering has become an important need for companies today to protect themselves against the proliferation of legal issues, adverse publicity and protect company property. If the companies aren't the smallest bit concerned about these major reasons, then they will soon realize it as it will begin to affect their bottomline.

References:

1. Internet Manager Web Inspector "Administrator's Guide" version 6.0. Jan. 17, 2003.URL: http://207.1.60.41/article.asp?article=10156&p=2(April 9, 2003)

2. In Sync Computer Solutions "Protecting Intellectual Property at 20th Century Fox" URL: http://www.insynclh.com/20thCenturyFox.htm(April 9, 2003)

3. Internet Manager Web Inspector "How to configure and deploy the UAM" November 25, 2002
URL: http://207.1.60.41/article.asp?article=10006&p=2(April 17, 2003)
Internet Manager Web Inspector "How to configure and use the LUA" December 11, 2002
URL: http://207.1.60.41/article.asp?article=10005&p=2(April 17, 2003)

4 Cohen, Sacha "Employee Surveillance: Where do you draw the line?" February 26, 2001 URL: http://www.itworld.com/Man/2690/IW010226cacop/(April 9, 2003)

5. Bloomberg News "Infoseek Executive arrested on solicitation charges" September 20, 1999.
URL: http://digitalcity.com.com/2100-1001-234891.html?tag=mainstry (April 9, 2003)

6 Pryma, Kristy "Monitoring for the 'sinful six' " January 30, 3003
URL: http://www.itworld.com/Man/2689/030130sinfulsix/page_1.html (April 9, 2003)

7. Phuoc Khanh, Truong, "S.F. police officer found dead in his car" December 7, 2002.
URL: http://www.bayarea.com/mld/bayarea/4692407.htm(April 9, 2003)

8. Internet Manager Web Inspector "Surftime, Accesses, Hits, Costs Explained" January 3, 2003.
URL: http://207.1.60.41/article.asp?article=10184&p=2(April 9, 2003)

9. Internet Manager Web Inspector "How does the SmartList™ Work?" January 8, 2003
URL: http://207.1.60.41/article.asp?article=10087&p=2 (April 9, 2003)

10. Internet Manager Web Inspector “Reports available in Web Inspector” November 11, 2002.
URL: http://207.1.60.41/article.asp?article=10025&p=2(April 9, 2003)

11. “JFK Medical Center Adds an Ounce of Prevention with Web Inspector”
URL: http://www.webcorrect.com.au/files/links/IM_JFK_Medical_Center_Case.pdf(April 9, 2003)

12. WebCorrect “IM Web Inspector Internet Monitoring Software” January 30, 2003
URL: http://www.webcorrect.com.au/pages/Elron(April 9, 2003)

13. Davis, Richard “Internet Abuse in the Workplace”
URL: http://www.victoriapoint.com/cyberslacking.htm(April 17, 2003)