GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Employee Monitoring: It is a fact, you are being monitored!

GSEC Practical Assignment
Version 1.4b
Option 1

Kimberly A. Bockman
March 9, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

In all industries in business today, computers and Information Technologies (IT) are a large part of the infrastructure. People in all departments from HR to Software development require a computer terminal and/or internet connection in order to do their jobs effectively. Even employees in the field are required to carry a laptop or some sort of handheld device to transmit information. This access to the world has introduced a number of new security related issues to the work force. One of the issues involves the company's right to maintain control over IT assets which provide employees with an avenue to silently perform personal activities. Employee monitoring is a very controversial topic; ranging from monitoring web access and keystrokes to installing biometric devices to monitor physical location and door entries. Based on the large number of monitoring tools on the market, employers are certainly monitoring employee internet activity. Understanding the employer's right to view an employee's internet activity and knowing what right to privacy an employee can expect at the work place will help to answer many of the questions around employee monitoring.

Introduction

Employee monitoring is occurring more and more frequently; many employees have no idea they are being monitored and if they did, like me, they would believe undisclosed monitoring of their actions to be a violation of their privacy. Whether an employer is watching her employees via the internet, the phone, or visually or accessing the equipment on an employee's desk (e.g. hard drives), employees and employers should know their rights and be aware of their legal positions as well as the rights of the employer to prosecute or release an employee based on this information. Knowledge of one's rights might prevent an employee from doing something (potentially innocently) that might threaten the company's assets or an employee's job. Also, it is important to note that legal rights typically have some gray areas and vary depending on the court and the interpretation of the laws.

As a result of this relatively new electronic security problem, many law suits and legal cases have developed with an employee believing they have a right to privacy while using company electronic data transfers and the internet. Knowledge of current laws and how they have been interpreted to protect the employer and company assets (in most cases) will help in understanding an individual's right (or lack there of) to privacy in the work place.

In addition to providing an overview of some of these laws and cases, this paper will discuss the right to privacy in the work place as it relates to the use of the corporate hardware, email, and internet access. It will answer the question of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

whether or not an employee even has a right to privacy in the workplace and it will address the issue of employee abuse of the company provided internet and associated statistics.

Finally, this article will describe several software tools available which were designed specifically to monitor employee computer and internet activity. These tools provide features like email monitoring (both content and viruses), internet web access (for personal web surfing), instant messenger use, and large file internet download monitoring. Using these tools will help a company accumulate data on how the internet resources are being used and which employees are guilty of using the corporate network for personal needs.

LAWS: Is there a right to IT privacy in the work place?

In a world where terrorist are using technology to threatening people and personal assets, industrial espionage is threatening trade secrets, and private data is placed in the hands of unsecured personnel, it is extremely important that laws protect the agencies holding these assets and information. Several U.S. laws have been established to help the corporate and government environments determine what their legal responsibility and actions should be if an incident occurs. Some interpretation of these laws takes into account the idea that monitoring can go too far and must also have some controls in place. There must be some control of monitoring in the workplace and especially control on the personal data being kept on the employees.

Privacy

The Federal Criminal Codes 18 U.S.C. § 2510 [1] and § 2511 [2] specifically discuss interception of wire, electronic, and oral communications. It is not always clear as to whether the laws are limited to personal homes or if the desk at the work place is considered personal property. Laws are subject to interpretation and the way one uses the law may vary (especially from state to state). It is not always clear as to whether the laws are limited to personal homes or if it crosses the boundaries into the workplace. A distinction should be made between "intercepting" information and viewing company stored data (in the case were an employer has a policy of storing on-line communications). The right to electronic privacy in the work place is limited by the definition of what is the company's property and what is personal property. The hardware assets are considered company property and the corporation has the right to access and confiscate the hardware when it is required, as was proven in the case *United States v. Simons,* where the company removed and replaced an employee's hard drive [3].

The Fourth Amendment is the standard "go to" policy in the constitution for a person's right to privacy. Interestingly privacy is not mentioned in the constitution but it does define the rights of a person against "unreasonable searches and seizures". [4] This is typically assumed to include home and personal property

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

but there are cases when a person's desk at work has been included in the realm of "personal property". Does this include internet access and electronic information at work? Is employee monitoring violating a person's right to privacy? The answer to these questions is "no". Employees do not have a right to privacy when it comes to electronic communications at work [5]. If an employer chooses not to monitor employees, they will be subject to potential lawsuits by employees if unacceptable content is transferred over their intranet and found offensive to someone in the workplace.

A law suit in 1990 *Shoars v. Epson America, Inc*, (http://www.law.seattleu.edu/fachome/chonm/cases/shoars.html) explains how an assumption of privacy in the workplace can lead to an unexpected dismissal from a position. Epson America had just introduced an email environment into the workplace and Alana Shoars was put in charge of encouraging all employees to use the corporate email system. After, explaining to employees that the system was completely secure and private (because it was password protected), Alana found that her boss had actually been intercepting the emails as they were being sent out. She was fired because of her stand on the subject and consequently filed a law suit against the company. Ultimately she lost the law suit because as the court put it "the employees should not have had any expectation of privacy"[6]. At the time of this lawsuit (1989-90), there were no laws on email use in the workplace but the result was the same as most employee monitoring law suits today and a false expectation of privacy led to an employee being released.

Employee vs. Corporate Rights

As mentioned many employees mistakenly believe that privacy is a right in the workplace. They believe that it is an invasion of privacy for an employer to track their activity on the internet. Several laws exist which can be used to define the rights of an employee and the rights of employers as they relate to privacy and employee monitoring. I am no lawyer and as I've found in my research, laws take many different forms depending on the US State and the interpretation. A couple of the laws found to be useful in lawsuits follow:

- The Civil Rights Act of 1964, Title VII provides the statement that has created the basis for many law suits. Title VII speaks of employment and discrimination. This gives an employee grounds to sue a company based on discrimination; including using electronic means to discriminate against an employee.
- The Electronic communications Privacy Act (ECPA) (1986) was developed to add electronic communications to the Federal wiretapping laws. This extends the protections to the transfer of an email and/or Internet use. In some cases this does not apply to the corporate environment.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Private sector companies as well as government organizations have many rights when it comes to the access and use of their corporate equipment. It is safe to say that laws are typically interpreted in the favor of the employer rather than in favor of the employee. The security of the company and the protection of its assets outweigh the needs for privacy in the workplace. Additionally, the company's argument in that it owns the computers on the desks and the network that the information is being passed over is extremely persuasive. As stated in the article Little Brother is watching you, by Miriam Schulman, "legally, employees have little recourse"[7].

Although, in most cases the company has a right to monitor its employees while on the job, the safest thing for an employer to do is develop a document that employees must sign stating they understand the rules of using the corporate internet. When a person joins a company, they should be required to understand the company's rules of behavior on the internet, possibly as part of the employee handbook. This will ensure that there is no misunderstanding of what occurs on the internet. Most companies don't mind if their employees do "some" personal internet surfing or if they use the corporate email for personal email (see statistics below). Personal use needs to be kept to a minimum and the company needs to assess the risks of completely eliminating personal use, causing disgruntled employees, against allowing unlimited access to internet use, making productivity go down.

A commonly sited case where employee monitoring of email was challenged in court is *Smyth v. The Pillsbury Company*, the company intercepted an email where Smyth threatened to kill people on the sales staff. When the employer intercepted the email and read the contents, Smyth was fired. Smyth felt his right to privacy was violated. However, the court found that Smyth had no reason to expect privacy in his workplace email unless some private information was included in the email. In this case you could argue that the email included personal information but the threat to other employees was a greater threat and the court found in favor of the Pillsbury Company [8].

Employee vs. Employer perspectives

Employers have more to worry about than employees wasting company time and resources to surf the internet, play computer games, or use company email space to send and store personal messages and data/music/picture files. Although those are legitimate problems, one of their largest problems is having employees who circulate inappropriate information over their networks. That information could result in multi-million dollar law suits for discrimination, sexual harassment, and other destructive reasons. The idea is that if an employer can be held liable for information circulated over their network, they must have some ability to monitor employees. What are their rights? When is monitoring going too far? And when is it not going far enough?

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

According to survey results accumulated by Vault.com [9], the following statistics about employee and employer perspectives have been accumulated from employers and employees:

Question	Employee's answer
How often do you surf non-work related web sites?	34.9% - a few times/week 38.1% - a few times/day 14.6% - constantly 12.4% - Never
How many non-work related emails do you send per day?	17.8% - None 56.3% - 1 - 5 12.4% - 6 - 10 6.3% - 11 - 20 7.2% - 21+
Do you think your employer is monitoring your internet and/or email usage?	53.5% - Yes 46.5% - No

Question	Employer's answer
What is the maximum amount of time an employee should be allowed to surf non-work related sites?	14.7% - Never 15.1% - Up to 10 minutes 34.8% - 10 to 30 minutes 24.9% - 30 minutes to 1 hour 5.2% - 1 to 2 hours 5.3% - Over 2 hours
Ho many personal emails should employees be allowed to send during the workday?	11.5% - None 53.6% - 1 to 5 17.5% - 6 to 10 6% - 11 to 20 11.4 % - 21+
Do you restrict/monitor your employee internet/email use?	41.5% - Yes 58.5% - No

Surprisingly, the employers and employees surveyed have similar opinions on what is considered acceptable use of the company's internet. While employers feel that employee monitoring is necessary in order to prevent events like, corporate information from leaving the organization and preventing employees from visiting web sites that are considered inappropriate, they also believe that for general use a little web surfing should be allowed. Employees apparently agree and continue to use the company's internet to for email and internet access.

Another organization, the American Management Association (AMA) has accumulated statistics in an article titled, 2003 Email Rules, Policies and Practices Survey, which describes percentages of companies who monitor

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

employee email activity. The article states that "more than half of U.S. companies engage in some form of email monitoring" and "enforce email polices with discipline or other methods". Additionally the article states that "1 in 20 companies has battled a workplace lawsuit triggered by email." [10] Proving that email security and regulation is a requirement in the workplace today. Employers are finding that when email is down the work place comes to a halt until it is back up. One large reason for email downtime is an employee receiving an email with potentially harmful attachments, which corrupt and/or bring down the email server. However, the downtime is balanced by the improved efficiency an employee sees because she has access to email which helps her do her job more effectively. Employers must understand and manage the risks and benefits associated with providing employees access to their corporate internet. Understanding that there is a balance and managing that balance effectively is part of the organization's requirements for success.

EMPLOYEE MONITORING TOOLS

Several tools exist to monitor employee activities, from simple operating system logs to complex multi-user monitoring software packages. These products provide employers with the information they need to get an idea of how employees spend their time at work. Many of them provide the employer with a mechanism for preventing users from accessing websites that have been prohibited by the company. According to the above mentioned AMA survey, 51% of the employers surveyed use software to monitor incoming email, 39% have software to monitor outgoing email and 19% monitor the email being sent from employee to employee [11]. Doing a quick search on the internet for Employee Internet Monitoring (EIM) finds that the market is flooded with products and tools (obviously a booming business). The following section describes some of the features of six randomly selected tools on the market today.

Websense Product Overview (http://www.websense.com)

Websense provides products in the areas of web filtering, network bandwidth optimization, monitors on instant messenger's ability to send files, and reporting tools which help the user analyze the data being accumulated during the monitoring process. This set of products is designed to help an organization manage the entire threat of internet abuse as well as potential outside threats like viruses and malicious mobile code (MMC). According to their website Websense is one of the most commonly used products for employee monitoring today.

An employer can use this product to track the amount of time an employee spends on the internet (personal and business). An employer could provide this information in the employee handbook to specifically outline the amount of allowable personal internet use and the type of sites that are restricted from use in the corporation. Having a tool like Websense will help define the rules and help both the employee and employer in the event of misuse.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A health care company sited on the Websense website, had a problem with network overhead and employees were having trouble doing their job because the internet was so slow. It turns out that employees were using the internet to download various types of files and to access their internet based email accounts. This was not only causing a drain on their bandwidth but was, among other things, allowing email based viruses to infiltrate their internet. The bandwidth and security issues are obvious here. This health care company was able to use the Websense software to prevent access to unnecessary websites, reduce the problem with email viruses and increase employee productivity [12].

ClearSwift MIMESweeper Product Overview (http://www.mimesweeper.com)

MimeSweeper is another widely known product on the market produced by ClearSwift Corporation. Their products protect a company against email threats such as viruses and spam. It also controls employee internet use and provides protection against internet email threats. MIMESweeper allows users to define "policies" that can be implemented on their network, providing time savings and lower set up costs.

Policies are a great way to establish a baseline of what is expected of employee's internet utilization. With an established policy an employee has no doubt what the rules are and what the corporate limits might be. By making policies available to the employees, the employer protects himself from having to define the line between what is acceptable and what is not acceptable after an incident has occurred. Having no gray area helps to defend against possible law suits that might arise from the lack of privacy in the work place.

In a case study located on the MIMEsweeper website, a major television manufacturer describes how MIMEsweeper was used to scan emails to see if any of the content was in violation of the company policy. In some cases the email could be held for inspection by someone on the staff or just deleted in the case of a virus. It is great for making sure viruses are not entering the company via email. The package cleans the infected file and frees up the IT staff to do more important tasks. Additionally, MIMEsweeper keeps data on the number of emails being sent out by various people to get some idea of where the resources are being used and/or abused. This product not only can help with viruses but it can also make sure email leaving the company abides by established polices[13].

SurfControl Product Overview (http://www.surfcontrol.com)

Surf Control has the ability to monitor content being downloaded to the company site by providing web filters, emails filters and instant messenger filters. Additionally, SurfControl helps with employee productivity by providing control over employees searching inappropriate websites. It also increases company

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

bandwidth by providing an ability to prevent downloads of large files like MP3s and videos. According to the website, it grossed the largest amount in revenue during 2003 of all the EIM tools researched.

Email is a crucial aspect of the work environment today. This is how employees keep in touch with customers, vendors, employees, and management. Having email is important but having control over the content is even more important. An employee could be leaking company sensitive information as well as sending jokes or crude emails that could lead to the company being sued. SurfControl provides the means for filtering and reviewing emails that might be sending threatening information over the corporate network. By informing employees of the corporate policy for monitoring email a company can see an increase in employee productivity and rest easy that their corporate secrets are not being distributed out of the corporate walls.

SurfControl not only provides email filtering but when more serious legal matters are involved like HIPAA compliance, SurfControl can provide a means for ensuring that confidential data will not be distributed through the internet via email. There is a lot legislation that defines how certain data is to be handled by the companies who keep that data and SurfControl can provide the means to be sure that those laws are kept and the data remains within the walls of the company and those with legal rights to the information [14].

Employee Monitoring Product Overview (www.employeemonitoring.net)

The product called Employee Monitoring (EM) is developed by a smaller company looking to attract smaller organizations which have less money to spend on employee productivity/monitoring tools but still wanting to provide a product with strong capabilities. Employee Monitoring has features like monitoring internet surfing and monitoring email for inappropriate or company confidential information. This product can monitor traffic on any port (not just the web). This enables the product to keep track of users who might be downloading large data files, music files, and/or pictures; causing throughput problems and slowing down the network.

In some companies it is imperative that all email traffic be recorded and able to be retrieved at a later time if necessary. This can be a company policy or in some government agency cases, it can be a court requirement. Products like EM are designed to record email traffic (including web based email) and provide a means for viewing the logs, extracting meaningful information, and reporting on that information. These features are crucial when trying to prevent certain types of messages from going out of the corporation and when trying to prevent unwanted emails from being distributed within the company.

A product like EM can help an employer keep track of employee productivity, network utilization, and email traffic. By allowing an employer to see what is

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

happening on the network, EM will increase employee output and decrease the need to build or create a more expensive infrastructure. As a product, EM has many interesting features. Customers referenced on their website seem happy with the results of the productivity being seen from their employees.

NetIntelligence Product Overview (http://www.netintelligence.com)

NetIntelligence (NI) is a network monitoring tool which also provides information relating to employee productivity. It helps to prevent hacking tools from being on company internet environment as well as denial of service utilities. NetIntelligence is a smaller lesser known product, advertised as having all the features of a larger monitoring tool.

A case study focused on the Employee Activity Monitoring aspect of NI, describes a large telecom company who needed to make sure employees where following their "Acceptable Use Policy (AUP)" and being productive while at work. Needing a system to monitor the employee's internet activity, the company implemented NI. After running NI on a sample group for a short time they found, among other things, that "almost 9%" of their employees were "surfing the internet almost ALL day". They were able to clean their corporate network of inappropriate material, free up disk space by removing unnecessary large files, and store information that could be used to punish employee misuse. [15]

Employee activity is not the only feature of NI, it also provides email and spam protection and an ability to keep illegal copyrighted data off the corporate network. NI is a very comprehensive product with many features that could bring security to a company's corporate internet. Visit NetIntelligence's website and you will find a number of reports detailing information and statistics about productivity, user activity, and web surfing.

Spy Anytime PC Spy Product Overview
(http://www.softlandmark.com/PCActivityMonitoring.htm)

PC Spy advertised on Soft LandMark's freeware website is used for both businesses and homes. Its inexpensive price makes it cost effective but its features are not as robust as the ones from the commercial products found on the market today. PC Spy provides the ability to monitor activity on a computer like file access, website interactions, email activity, internet chats, and passwords. All of these activities are monitored without the knowledge of the employee (or person).

Spy Anytime is advertised as an "employee monitoring" tool but after reading about it and going through its website, it seems to be more of a small time home monitoring tool for children or spouses. It can be used as a corporate tool but probably for a smaller company that needs a product to give them some idea of how their internet assets are being used. For a large corporation, they would

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

need something that provides a good reporting tool and even an ability to do some self correcting or on the spot learning (building a database of information that is considered “unacceptable”).

Product Tools Summary

The products described provide many of the same features. A user can build filters which can clue the company in to corporate internet abuse or unsavory website activity. Many companies are beginning to incorporate employee monitoring tools into their network and LAN administration tool sets. In some cases they are accumulating data that they might need to retrieve at a later time and in other cases they looking at specific people who might be using the corporate LAN to find distasteful websites or build their own music storage space. Whatever the case, employee monitoring tools are popular and have many features that could help an organization keep track of employee activity. Software tools are providing the means for employers to gather the information they need about their employees’ use of the corporate internet. The data can be useful in extreme cases but having the employees know that they are being watched increases productivity considerably and reduces the security risks associated with employee internet surfing. Some organizations choose not to let employees know they are being monitored, in either case employees have a high probability of being watched and should be aware of the potential.

CONCLUSIONS AND PERSPECTIVES

When I began researching this topic, I thought I understood the security issues with providing internet and email access to employees. I felt pretty strongly that the company would need a reason to access any of my internet communications (or desktop activity) and then use them against me if something security related happened. A right to privacy, in my opinion, was necessary even at my desk at work. I occasionally make personal phone calls from my desk so why can I not send out personal emails and instant messages? As I started reading articles, legal accounts, and books on the subject, I started to see a different perspective and understood that my original opinion on the subject was wrong. It is not safe to assume that no one is watching me, as a matter of fact it is very likely that someone is at the least filtering on key words during my internet access and it is assured that my email messages are being stored somewhere (evidenced by the fact that when I had a hard drive failure, they were able to recover any email that I maintained on the server and several of the emails that I copied to my hard drive or deleted).

The employer has provided their employees with equipment and access in order to do the job that they were hired to do; and legally the hardware assets and corporate network is their property. Many fine lines and grey areas still exist and most companies seem to be avoiding the potential problem by providing written contracts stating the rules for electronic communications as well as on-line

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

behavior. These documents are typically signed by the employee consenting to the monitoring and being made aware of the potential or likelihood. These documents also define what "acceptable use" is. In other words, if they allow personal access, they specifically list the number of emails and employee can send out each day or week as well as the number of recipients a personal email may have. Some companies say it's okay to surf the internet during off hours or for a specified amount of time each day. Having this information can ensure that an employee knows the limits and that they will have to pay the price if those limits are exceeded.

Realistically, no company could actually "watch" every employee without spending far more money on the equipment to do so than they are saving in employee productivity. But after researching the employee monitoring tools available on the market today, it's fairly easy for companies to build filters and search for key words that might be offensive or prove that proprietary corporate information is flowing out. Based on the growing market of employee monitoring tools, companies are purchasing and using monitoring tools to monitor employees; this information can be used against an employee if necessary.

After reading the list of "Surprising Internet Use Statistics" from the Websense web site (http://www.websense.com/products/why/stats.cfm), it is apparent that employee monitoring could help to increase productivity. Many companies don't mind a limited amount of web surfing or internet communication but there has to be a balance between a 5 minute escape and spending half a day shopping on the internet. Employers are entitled to make sure their employees are providing "an honest days work for an honest days pay" as well as making sure their corporate proprietary data is safe from distribution outside the corporate walls.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

[1] Federal Criminal Codes 18 U.S.C. § 2510, http://www.usdoj.gov/criminal/cybercrime/wiretap2510_2522.htm

[2] Federal Criminal Codes 18 U.S.C. § 2511, http://www.usdoj.gov/criminal/cybercrime/usc2511.htm

[3] Case 9-1: Privacy, United States v. Simons, http://august1.com/courses/cyber/cases/Simons.htm

[4] Alderman, Ellen and Caroline Kennedy. The Right to Privacy. New York: Vintage Books, 1997. p.10.

[5] Muhl, Charles J. "Workplace email and Internet use: employees and employers beware". Monthly Labor Review. February 2003. http://www.bls.gov/opub/mlr/2003/02/art3full.pdf

[6] Alderman, Ellen and Caroline Kennedy. The Right to Privacy. New York: Vintage Books, 1997. p.310 – 317.

[7] Schulman, Miriam. "Little Brother is watching you". Issues in Ethics, Spring 1998. http://www.scu.edu/ethics/publications/iie/v9n2/brother.html

[8] C.A. No. 95-5712, Michael A. Smyth v. The Pillsbury Company, 1996 http://www.loundy.com/CASES/Smyth_v_Pillsbury.html

[9] "Results of Vault Survey of Internet Use in the Workplace", Survey Results, http://www.vault.com/surveys/internetuse2000/index2000.jsp

[10] [11]American Management Association, "2003 Email Rules, Policies and Practices Survey". http://www.amanet.org/research/pdfs/Email_Policies_Practices.pdf

[12] Websense Case Studies, "… Fights Network Infection and Bandwidth Growing Pains with Websense", http://www.websense.com/products/why/casestudies/mercyhealth.cfm

[13] MimeSweeper Case Studies http://www.mimesweeper.com/download/collateral/casestudies.aspx

[14] SurfControl Website, "Assessing the Risks", http://www.surfcontrol.com/industry_solution/healthcare/hc3.aspx

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

[15] Netintelligence Case Studies, "Employee Activity Management Case Study", http://www.netintelligence.com/employee%20activity%20management%20casestudy.htm

Joel, Lewin G. Every Employee's Guide to the Law. New York: Pantheon Books, 1996.

Lane, Frederick S. The Naked Employee. American Management Association, 2003.

Burke, Christiansen, and Kolody. "Emerging Threats to the Employee Computing Environment", IDC. http://www.idc.com

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.