Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Content Monitoring Issues Legal and Otherwise

We will begin with a brief discussion of the broad types of monitoring that occur as well the motivations and potential issues involved. Then the main laws relevant to employee monitoring will be summarized along with some sample cases resulting from this legislation. Finally, a set of best practices will be suggested with a focus on keeping the company out of trouble.

Copyright SANS Institute

Author Retains Full Rights

AD

DEEPARMOR®

GLEG Gold Certification

Author: Darryl T. Barnes, darryl.barnes@yahoo.com

Adviser: Dominicus Adriyanto

Accepted: February 22nd 2009

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Outline

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

1. Abstract

If you are in IT security, then you are probably involved in monitoring employee content. There is a plethora of land mines surrounding this activity. Do you understand the issues? Do you understand the legal underpinnings behind your snooping? Most articles on this subject are superficial in their coverage, and most are written from the perspective of the employee and their privacy. This paper is written from the perspective of the IT security professional. And while a single paper cannot thoroughly examine every aspect of this topic, many areas are covered including an examination of the issues, a review of federal and case law, a set of best practices, and things that could get you in trouble. Everyone should learn something pragmatic and useful in this paper.

2. Introduction

With the advent of the Internet, companies have an increased need to monitor their networks for external compromises and as well as inappropriate use on the part of their own employees. This paper looks at the risks and issues related to the electronic monitoring of employees by corporations under United States law. The intent is to provide awareness of issues involved with employee monitoring and to suggest some best practices.

There has been quite a bit of material written on employee privacy from the employee

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

perspective; however, this paper is written from the perspective of the employer. The primary audience is IT security management personnel who are involved with monitoring employee activity, and the typical technical level of an IT professional is assumed. Please note that industry specific laws and issues as well as state specific laws are not addressed.

We will begin with a brief discussion of the broad types of monitoring that occur as well the motivations and potential issues involved. Then the main laws relevant to employee monitoring will be summarized along with some sample cases resulting from this legislation. Finally, a set of best practices will be suggested with a focus on keeping the company out of trouble.

3. What is Content Monitoring?

Content monitoring is a form of electronic monitoring. Electronic monitoring covers a very broad range of activities including: content monitoring, video cameras, phone ease dropping, and location tracking.

" ''Electronic monitoring'' means the collection of individually identifiable information concerning employee activities or communications through the use of an electronic device including, but not limited to, a computer , computer software or other computer program,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

telephone, wire, radio, camera, or electromagnetic, photo-electronic, or photo-optical system (California Senate Bill No. 1841, 2004)."

With content monitoring we are strictly concerned with information either on an employee's computer or that is being sent over the network. IT security personnel can potentially monitor many aspects of an employees computing activities. These may include:

- Contents of files and application programs located on a computer
- Web traffic
- Email content stored on in-house email servers
- Email content being sent over the network to outside email servers
- Flow data (system to system communication within a network)
- Full network traffic capture
- Computer forensics analysis
- Instant messages (IM)
- Screen captures on a computer while an employee is working
- Keystrokes

The most typical content monitoring activities are web access, email, and direct

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

computer access. Since most companies host their own email server, searching company email is a straightforward task. Monitoring web access requires additional infrastructure. The most common for large companies is a network based web proxy solution such as those from Bluecoat.

Encrypted web and email content cannot be monitored unless the network has an SSL proxy installed, which is relatively uncommon. An SSL proxy acts as an "man in the middle" intermediary that separately encrypts the session between it and the client and itself and the target system, thus allowing the proxy to see all traffic that passes through it in the clear. This only works for server-only authenticated sessions. Mutually authenticated sessions are generally not allowed through the proxy gateway since they cannot be intermediated.

In general, content monitoring is accomplished using a central server (or network appliance) or a combination of client agent and central server depending on the goal. For instance, flow monitoring is accomplished using a network appliance that integrates into the router and switch fabric. Keystroke monitoring and screen capture would require a client agent that transmits the captured information to a central server for storage and retrieval. Keystroke and screen capture capabilities are considered highly intrusive and are not commonly used in larger corporations, however, these capabilities are common in small business employee surveillance applications.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Full network capture and flow monitoring capabilities are typically used exclusively be large corporations. These systems are network-based appliances that tap into the core network infrastructure. Full network capture solutions require a very large amount of disk space which usually is configured to overwrite itself once consumed. Ideally, several weeks or more of data will be stored at a time. This data can then be analyzed in real-time, potentially triggering preset alerts, or later for ad hoc queries.

Flow data is collected from the router and switch fabric. It can show computer-to-computer communications including ports, protocols, and often some initial content. This can be very useful information for both misuse and for various security incidents. If you know a computer was compromised, you can then see what other computers have been accessed and therefore may be infected. You could also see what systems an insider threat may has been accessing.

Forensics analysis tools provide the capability to do detailed analysis of a computer hard drive. Forensics tools are not real-time monitoring tools and so one could argue that they are a separate animal; however, they are used to view employee data. Of special interest is the ability to recover deleted files that the employee may have thought were really gone. This is reminiscent of the technical naivety of Colonel Oliver North who thought he deleted evidence of Iran-Contra affair when he hit the delete key only to have them come

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

back to haunt him in court. These tools can typically create images of disks with a checksum, perform browsing, and data recovery. These are important capabilities for the detailed investigation of a compromise and in the collection and preservation of evidence for potential prosecution.

All of these capabilities create a tool set for the IT security team. This tool set enables them to proactively detect unwanted behavior and intrusion, as well as provide post incident research and forensics. However, in addition to the technical understanding of how to use these tools, team members need to understand the legal ramifications of their use in order to be effective and avoid missteps.

4. Why Do Content Monitoring?

The American Management Association conducts a yearly survey of US company's monitoring and surveillance policies. A full two-thirds (66%) of all employers now monitor web usage, and 43% monitor email content. Nearly all companies are concerned with the visitation of adult content sites while only about one third are concerned with excessive personal usage of the web. (AMA ePolicy Institute Research, 2007)

Corporations generally monitor their employees for four primary reasons: litigation

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

avoidance, data leak protection, productivity monitoring, and compliance. Which one is the primary driver depends greatly on the type of business and can even vary based on the type of employee (e.g. upper management vs. customer support).

A company whose employees are primarily knowledge workers and have a great deal of intellectual property should be very concerned with data leak prevention. In most cases, their employees have access to the Internet as well as portions of the company's intellectual property. The insider threat for this company poses a significant security risk.

On the other hand, a company that is an outsource provider of customer support with a high turn-over rate may be primary concerned with productivity. As a result, they may take random screen shots to assist in gauging individual productivity.

For example, one Silicon Valley biotech firm employed lab technicians that used shared computers. At least one of the male technicians accessed pornography on a regular basis, which was often discovered by one of the female technicians who used the same shared computer. There was valid concern that this inappropriate use might result in a hostile workforce claim by the female technician. In this case, litigation avoidance was the driving factor in the web usage monitoring that took place after that incident.

A common term associated with monitoring is "inappropriate use". The term generally applies to pornography, gambling, hate, hacker content, and shopping. A company may

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

justify blocking these types of sites based on productivity or litigation concerns. An additional concern is that the threat vector for some malware is via HTTP which could result in data compromises. It is true that frequenting adult content sites results in a greater risk to infection. However, with the advent of dynamic web-based attacks (a.k.a. "drive-by downloads") more and more legitimate sites are being compromised and are the source of malware (Provos et al., 2008, pp. 9-10)

What a particular company or individual considers inappropriate is completely subjective. For some companies, inappropriate use can be anything non-business related. So, checking the latest headlines and stock quotes might also fall into this category. On the other hand, a memo sent out by a senior security manager at one federal agency stated "that we (security professionals) are not the morality police". This manager's view was that if it didn't represent a direct security threat, then it should not be addressed by security. This is a good line to draw for the security team. Unless there is direct guidance from upper management that something is inappropriate, and if there is not direct threat, then no action should be taken. This approach removes a lot of ambiguity for the security team.

One of the big drivers for content monitoring is the avoidance of lawsuits. Employees can harass each other via email and IM. Pornography can be viewed on shared computing resources which can create a hostile work environment. These are real issues that involve

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

the protection of employees. By not performing any monitoring, you are not addressing this risk of litigation directly. Policy alone will not sufficiently mitigate this risk. The courts have often made judgments against companies based on the fact that they SHOULD have known of the abuse if the abuse was deemed flagrant enough.

5. Issues with Content Monitoring

Employee Morale

The effects of monitoring on employees can be as varied as the methods used. Strict monitoring of productivity may cause recurring stress in some people, which may, in turn, increase turnover and absenteeism (National Workrights Institute, n.d., p.5 para. 1). Certainly people under stress are less cordial and friendly. If an employee is customer facing, then customers may sense the stress and get a negative impression. Another risk is from employees attempting to "game the system" by playing only to the metric, which may have unintended consequences.

Managers should also consider the effects on moral and culture. The amount of employee monitoring sends a strong message to employees regarding the level of trust company management has in them. Monitoring that is relatively strict may produce an "us" versus "them" mentality in many employees. On the other hand, people do have an

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

understanding of the need for justified restrictions. Striking a balance between what could be done and what should be done should be carefully considered.

Whatever is done needs to be communicated and justified in the open. Manipulation and mistrust comes from closed agendas. A company has the right to expect productivity from its employees, take steps to avoid litigation, and to protect its intellectual property. The laws of this country fully support this view and generally lean toward the company's rights versus the privacy rights of employees; however, trust once broken is hard to mend. The way to build and maintain trust is be open. Open as to what is being monitored and why.

Trust Level of Monitoring Team

Many positions within a corporation are sensitive due to access to information, physical access, or being a position of power. Some examples are finance positions, HR, and security guards. Some companies perform enhanced security checks on these positions. IT security operations, on the other hand, has tremendous access to sensitive information but rarely goes through any enhanced vetting. Your local cyber criminal also happens to be extremely well qualified for that security analyst position. Just reading the job posting let alone interviewing for the position can provide a wealth of intelligence on a company. There may be no limit to what they can do once inside.

Most IT security analysts are in a position to (1) monitor critical business

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

communications, (2) harass another employee (in a much more sophisticated manner than the average employee and that would be hard to detect), (3) their specialized knowledge puts them into an excellent position to pilfer intellectual property and actual funds, and (4) put someone in jail with what they discover and the evidence that they collect. Clearly this is a position of sensitivity and should be treated as such. Some controls are suggested at the end of this paper.

Defining Objectionable Content

Objectionable is subjective. For instance, what is pornographic? The answer is probably going to be quite different from a 60 year old female with a conservation religious background versus a 30 year old male whose parents were hippies. What about hate, jokes of poor taste, and cuss words?

The author once had a co-worker that would complain to management every time she heard a cuss word regardless of context. She was largely ignored simply because she was in the extreme minority. This illustrates that the composition of a group and specifically the composition of the group in charge determines the definition of objectionable. And clearly, social morals shift continually over time. Society has reacted to this complex issue by creating a high watermark and making nearly everything “politically incorrect”. There is no clear solution to these issues; however, there are often risks when applying real enforcement

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

against any given morality standard. Who determines the standard? Who applies the standard? Is it really going to be applied consistently in all cases?

One area in which there is consensus is child pornography. As a society we have chosen a broad view of child pornography because children are unwitting participants and require special protections. Even so, there will be grey areas in which a determination must be made and people who must review the material. As a result, somewhere out there is a group of law enforcement professionals that don't sleep at night, and children are saved as a result.

Targeted monitoring

Targeted monitoring is an issue associated with employee monitoring. It occurs when an employee is picked out specifically for monitoring under a set of rules that is different than what is used for other employees. The motivation can vary greatly and may include a desire for retribution, prejudice/dislike, jealousy, unrequited affection, or fishing for a reason to terminate someone. The dangers here are the abuse of power and the creation of inequalities in the workplace. Besides being patently unfair, it creates litigation risk. A fired employees could claim wrongful termination based on discrimination, or in the case of unrequited affections, an employee might claim a hostile work environment.

One should watch the perception of targeting due to inconsistent application of policy.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

For instance, the security operations team may not be applying it's operating procedures consistently. The procedure may state a threshold of ten or more large (non-thumbnail) pornographic images discovered during a given week before investigating. In one particular case, they may decide to investigate after only three images were found, and in turn, find a large cache of inappropriate images. If this person is terminated, they may be able to fight the termination claiming that they were unfairly targeted. When a company treats employees differently it must be prepared to show why or risk litigation (Candris, 2007).

6. Federal Laws

Computer crime is a relatively new phenomena within the legal realm. However, wiretapping is an analogous activity to content monitoring and has been around for many decades. Early cases concerning privacy of employees within the workplace relied on examples of an expectation of privacy derived from judicial precedent on wiretapping. For example, the 1929 supreme court decision Olmstead v. United States that ruled that telephone wiretapping by the government did not violate the 4th amendment. A decision that was subsequently reversed in Katz v. United States in 1967 (Olmstead v. United States, 1928).

Much of the legislation in place has focused on protecting citizens from the prying eyes

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

of government and has failed to address private corporations. Most legislation that does focus on corporations focuses on protecting customer information, for instance, the Children's Online Privacy Protection Act (COPA) and the Health Insurance Portability and Accountability Act (HIPAA). At a high-level there are still many areas that are not addressed by the courts. What law does exist is often conflicting. For instance, US v. Councilman where the 1st Circuit reserved ITSELF with regard to whether email temporarily stored while in transit to its final destination violates the federal Wiretap Act (United States v. Councilman, n.d., p.1).

The core set of federal legislation that is relevant to the monitoring of employee content is the:

- 4th Amendment
- Computer Fraud & Abuse Act (CFAA)
- Wiretap Act
- Electronic Communication Privacy Act

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Fourth Amendment

The Constitution does not guarantee a "right to privacy", but it does place safeguards against government invasion of privacy (BBBOnLine, 2008, p. 1). The foundation of all US law regarding wiretapping and unlawful search is the Fourth Amendment of the Constitution, which states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment was not always applied to wire communications, however. Not until the landmark Berger v. New York (1967) did the Supreme Court apply the Fourth Amendment and lay down requirements for the constitutionality of interception orders by the government (Monnat & Ethen, 2004, p.12).

These requirements included probable cause, that warrants must describe the who how and where of the search, have reasonable scope and execution, provide post-execution notice and return. A second Supreme Court decision (Katz v. United States) extended the Fourth Amendment protection from unreasonable search and seizure to protect calls in a telephone booth from wiretaps without a warrant. This case declared that the Fourth

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Amendment protects people and not places (e.g. home) ("Katz v. United States, n.d., para. 1).

The Fourth Amendment only directly applies toward protecting citizens from government intrusion; however, it is relevant to cases of corporate monitoring of employees because it is the foundation of many privacy arguments including the objectively reasonable expectation of privacy. For instance, in the United States v. Simons (2000) it was reasoned that an employer's Internet-usage policy defeated any expectation of privacy (United States v. Simons, n.d., p.1). This reasoning has been extended to most cases involving private companies.

Wiretap Act

Congress reacted to these decisions by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which is generally referred to as the federal Wiretap Act. This legislation sought to enact statutory wiretapping rules that satisfied Berger v. New York. It imposes civil and criminal liability for 1) intentionally intercepting wire, oral, or electronic communications; 2) attempting to use a wiretapping device; 3) using or disclosing the contents received through wiretapping; 4) and disclosing lawfully intercepted communications in order to impede a criminal investigation. (Monnat & Ethen, 2004, p.13).

The federal Wiretap Act provides for a list of exceptions. For example, if one of the parties to the communication has given prior consent, interceptions by services providers

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

within their normal course of business, or interceptions of communications from a compromised system by a computer hacker (Prosecuting Computer Crimes, 2007, Sect. A5).

Note that while the Wiretap Act addresses electronic communications, it doesn't specifically address computer data. In addition, it addresses transmissions and not the storage of those transmissions. This makes sense from the historical view of telephone transmissions, however, provides little protection in the case of email communications.

Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 (ECPA) contains two major components. Title I amends the federal Wiretap Act which addresses electronic communications. The second component (Title II) is called the Stored Communications Act (SCA), and it addresses data in intermediate storage. The Wiretap Act primarily evolved from court cases addressing the tapping of phone lines. And although it did address electronic communications, its lack of specificity caused issues in obtaining convictions regarding the tampering of computer systems. The purpose of the ECPA was to modernize the Wiretap Act to address modern computing and specifically electronic data. This was primarily accomplished through the addition of the Stored Communications Act (Electronic Communications Privacy Act, n.d., paras. 1-4).

The SCA protects communications held in intermediate storage, and so before the

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

intended receiver takes ownership. It defines unlawful access to stored communications as "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system" (Electronic Communications Privacy Act, n.d., section 2701).

Violations of the SCA are significantly less severe than the Wiretap Act. This is relevant as the court system struggled as to whether to apply either the Wiretap Act or the SCA to Internet communications.

Computer Fraud & Abuse Act

The Computer Fraud & Abuse Act (CFAA) was passed in 1986 to create a distinct law for the prosecution of computer crimes. It has been amended many times since it was created in order to clarify language, such the definition of a "protected computer", and strengthen sentencing provisions (CFAA, n.d., p. 1).

The CFAA defines protected computers as those exclusively used by financial institutions, US government systems, and those used in interstate or foreign commerce or communication. The last category encompasses pretty much every computer connected to the Internet.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The CFAA forbids intentionally accessing a protected computer without authorization and:

- Obtaining anything of value
- Committing fraud
- Causing damage
- Trafficking in passwords
- Committing extortion by threatening to cause damage

(Computer Fraud and Abuse Act, 1986)

The act goes into more detail about specific types of records that are protected such as, government records, financial institution data, and classified information. In some cases, the penalties vary according to the type of record.

The act also distinguishes between an insider who exceeds authorization from an outsider who is unauthorized. Specifically, an insider is not criminally liable for negligently causing damage, but is liable when accessing with intent to defraud and obtain value. On the other hand, an outsider is held liable in all cases of damage (Prosecuting Computer Crimes, n.d., ch.1 p.4). However, there have been cases whereby an insider was held to have acted without authorization in certain actions that were excessive. Damage must exceed $5000,

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

but time spent investigating and repairing the system can be included. As a result, most any compromise to a business system would meet the minimum damage requirement.

Proposed Legislation

There have been attempts at legislation, proposed both at the federal and state level, that directly addresses employee monitoring. In 2000, the Notice of Electronic Monitoring Act (NEMA) was proposed by the US Congress, which would have required stringent notice requirement on employers. Basic notice requirement laws have been passed by both Delaware and Connecticut. In 2004, California bill SB 1841 Electronic Monitoring of Employees was vetoed by the California governor. This bill specified very specific notice requirements and rejected, for instance, notice by logon banners as not sufficient (California Senate Bill No. 1841, 2004, Section 1). It is likely that additional legislation will continue to be passed at the state level and quit possible at the federal level.

7. What Might Get You In Trouble

The following are some areas that you should be aware of that legal grey areas. On these issues proceed with caution.

Alternate Telephones

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Telephone communications are generally subject to tighter restrictions than computer use. Courts allow for a greater expectation of privacy for phone calls. Even the NSA provides a greater degree of notice to its employees by placing a monitoring notice on every phone handset. Although there is little to no judicial history for the specific subtleties of VoIP equipment or Internet telephony, clearly this is a grey area in which a company should proceed with great caution.

With the advent of VoIP, companies have a greater opportunity to tap employee phone conversations, and this communication is now travelling over company networks and equipment. Is it now more like an email since it travels over the same company network? Or are there no differences to a standard Plain Old Telephone Service (POTS) phone with all of the same rules and restrictions? In this case, one should act with extreme caution. The primary argument will be that since it looks like a regular phone and acts like a regular phone, then it should be treated like a regular phone.

Internet phones (e.g. Skype) are fundamentally different. In most all cases, the employee will have setup the Internet phone on his own. Also, in most cases, the interface is very different than a POTS phone (i.e. headset). And finally, the Internet is clearly connected to a computer. One now has several degrees of separation from the general telephone experience. It is much more likely that a court will see the monitoring of an employee setup

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Internet phone as falling under the same guidelines as other Internet communications. So, assuming that Internet phone monitoring is stated within you monitoring policy, monitoring your employee's Internet phone *might* not get you in trouble.

External Resources

Most court cases have decided with companies with regard to the monitoring of employee email. Nevertheless, there are grey areas within email monitoring. What about personal email accounts accessed over a home network but stored on a company computer? What about personal email sniffed off the corporate network that are destined for the employee's personal computer? An email containing company trade secrets was sent to an employee's personal account. Your team has captured the logon credentials. Can you go delete the message before it's accessed externally?

Perhaps in a hundred years all of these scenarios will have been definitively addressed by the court system. Today, however, each of these scenarios presents potential issues. The core issue is when is it appropriate to read or access an employees personal email account. There have been courts cases that supported allowing a company to review personal email stored on the companies computer, even when the contents are password protected.

Do you have the right to access the text messages on your employees company

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

provided mobile phone? In Quon v. Arch Wireless the court said that a police department did not have that right, and that the police officer had a reasonable expectation of privacy (Gordon, 2007, para. 4). Note that it was the phone company that got sued and not the police department. When your company does not operate any given service itself, then there is risk that an expectation of privacy argument will succeed. The growth of outsourcing of IT services may create barriers to a company's ability to monitor employee activity.

Capturing personal email account credentials on the corporate network and the accessing that account would be a violation of the EPCA since the company would no longer have the cover of the service provider exception. It's very likely that even if you are sure of theft that breaking into the external account will land you in hot water. This is a case where knowing your law enforcement colleagues in advance will be very helpful.

Acting on information found in an email sent to an employee from a non-employee in a dual notice state is fraught with trouble since you likely have no notice from the sender. Clearly, the only legitimate reason to act might be if the person was suspected of doing something illegal. If the sender sent child pornography, then the mandatory FBI notification would come into effect. You would get in more trouble by not acting and the moral justification would be clear. Legal council should be sought in any situation involving non-employee content.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

8. Best Practice

The following is a set of best practices that address some of the issues that have been brought up within the paper.

Providing Notice

As previously discussed, the ECPA requires that at least one party to a wiretap be notified. Within a corporate environment this is generally accomplished in one of two ways. First, the explicit signing of a statement that you have read the monitoring policy (or employee handbook that contains the policy). Ideally, this policy should be broad and specific at the same time. The second is a logon banner that states that one should have no expectation of privacy on this network, etc. A third frequently used method is an annual IT security training presentation or online training.

Knowledge of this requirement is well known within the IT security community. Discussion on this subject is usually more about implementation details. In fact, most companies do provide employees notification. According to the AMA survey 83% of employers notify their employees that they monitor content. Although only 27% of companies integrate this into formal training (2007 Electronic Monitoring & Surveillance Survey, (2007), p.2).

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Targeted Monitoring

Targeted monitoring is a litigation risk. Your organization should consider controls to mitigate this risk. Two possible controls are outsourcing and separation of duties.

Most of the motivations for targeted monitoring requires that the person doing the monitoring knows who the target of the monitoring is. If the monitoring personnel are not part of your organization, then they should not know John Doe from Jack Frost, and hence, unlikely to specifically target either. Therefore, outsourcing of the monitoring personnel is an effective mitigation. This does not stop someone from your organization requesting the special monitoring of a specific person, and so policy is still required for the third party monitoring team to ensure proper authorization of these cases. That policy may require notification of others within upper management or HR, for example.

A second mitigating control with regard to targeted monitoring is the separation of duties. Assuming a large enough organization, you could have two tiers of incident investigation. The first tier does the initial capturing of the incident and perhaps entering it into an incident management system, then the second tier performs the incident analysis. If possible do not allow access to the IP/employee mapping information. Ideally, this would only be accessible by the team manager.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Vetting of Security Operations Team

Another best practice area is vetting and monitoring of the security operations team that performs the employee monitoring. There is a real business risk associate with the power and capabilities of this group.

Companies need to put controls in place that mitigate the special risks associated with their security operations teams. Two controls were just discussed with regards to targeted monitoring. Namely, outsourcing the monitoring team and separation of duties.

In addition, security operations teams should be subjected to enhanced background checks. Some available options are criminal, credit, public records, drug testing, and driving record checks. A private investigator can be hired to look deeper into the employee's background. Association with criminals and black hat types would be warning flags. Within the government, some clearance levels require polygraph evaluations; however, due to the Employee Polygraph Protection Act, this is not an option for private employers (U.S. Department of Labor, 2008, p.1).

Controls should be in place to audit the activities on the content monitoring team. First, their activities need to be logged to the degree practically possible. Second, access to the audit logs need to be exclusive to a separate administration team. It is pointless to have an audit trail that can be altered by the people that are being audited. It is very likely that the

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

security operations team will have knowledge of what is being logged, and due to their deep understanding of the network will know ways around these measures. Therefore, there should not be a false sense of security due to the mere existence of audit logs.

Disclosure and Least Invasive Method

In some parts of the world, laws have been enacted that require companies to use the least invasive method to achieve a desired result. For example, within the UK the Data Protection Act of 1998 addresses workplace monitoring. The law recognizes that businesses have legitimate needs to utilize monitoring of their employee. These laws require that the business state in writing that the need is legitimate and that the monitoring is justified to meet the need. In addition, the monitoring method must be shown to be the least invasive method to address the given risk (Heydary, 2005, para. 18).

This type of assessment method isn't required in the US, at least not yet. However, it is an excellent control against monitoring abuse. By forcing the security team to justify their practices in this manner, it forces the team to think through, in detail, each of their monitoring practices. You do not want an out of control IT security staff overstepping their bounds and pushing the limits on monitoring. In an ambiguous environment they may feel that they can justify anything, which increases the risk of litigation or even damage litigation against some legitimate wrongdoer. Open and explicit policies will go a long way in keep any renegade

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

security person in check.

In addition, these laws as well as several proposed (but un-passed) laws within the US have required explicit disclosure of monitoring practices. From a security professional's perspective, there is value in the uncertainty of the user community as to exactly what is being monitored. By being on the secretive side, you can create the impression that every conceivable thing is being monitored when in fact it's not, and this may discourage some behaviors.

But the fact is there a great deal of legal grey area around employee monitoring, and it is in the best interest on the company to stay within the clearly defined boundaries as much as possible in order to reduce the risk of privacy infringement related lawsuits. Whereas the courts generally side with the employer regarding the right to monitor, the legislative trend is toward full disclosure. By moving toward full disclosure now, your company will have plenty of time to put these measures in the place.

IT security isn't the secret police. If you allow a negative dynamic to develop between an unfettered monitoring team versus the fearfully monitored users, then you are likely to get unintended resistance and mistrust of management in general. Fear is an effective control mechanism, but controlling employees isn't the end goal, productivity is. Fearful employees may react in unpredictable and often unproductive ways. For instance, they may start to take

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

an “us vs. them” approach to management and resist even the most benign management practices.

Defining Abuse

As stated, defining what constitutes abuse can be a slippery slope. However, it is important that policy is put into place that sets some limits on acceptable online behavior. The following is some best practices regarding this policy. First, it is best to clearly define, when possible, what is deemed objectionable by the company. Secondly, it is important to define who has the final call on what is objectionable. And lastly, it is imperative that whatever implicit or explicit policy is established, is applied consistently across the company.

Another good practice is to have an SOP that explicitly defines potential abuses. A categorization system for potential abuses is a good approach here. Categories may include: non-abuse, non-actionable abuse, actionable abuse, and criminal abuse. Non-abuse would be anything not explicitly defined as abuse.

Your company’s Internet use policy may state that reasonable use is permitted, however, it’s unlikely that the policy defines what reasonable use is. The IT security operations team needs to know when to act and how. It might be determined that reasonable personal use ends after one hour, and that one to two hours is considered non-actionable abuse that is simply recorded. Anything over two hours may be escalated to the employee’s

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

direct manager along with all non-actionable abuse reports. Clearly, no amount of goofing off could be considered criminal abuse. Examples of potential criminal abuse includes child pornography, hate content, and threats against others. Good practice would be to require immediate notification to upper management in all potential cases of criminal abuse.

Contents of the SOP should be reviewed by upper management, HR, Legal, and IT security management. Considerations may be to reference the abuse SOP within the Internet use policy and making it available upon request, or even publishing it on an internal web site.

9. Conclusion

It is important to remember that, at the end of the day, company employees are people. As an IT security professional you often have special privileges with regard to access to information about other people similar to HR. What you do with that information effects peoples lives for good or bad. Your attitude toward them, due to your position, will effect their morale and their attitude toward other IT security controls and even management. You should take this privilege seriously and respect it. For often a lack of respect for the people within your domain of responsibility is exactly what will get you in trouble.

If you are hiring people for the security team you should consider this when considering the candidates. Probe for their sense of right and wrong. Their level of maturity.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Observe if they are humble or arrogant. Ask them ethical questions with no clear answer and ask for their thought process when working through the problem. In short, choose carefully and do your due diligence.

A lot of material was covered within this paper and many ideas were discussed. The legal environment will continue to change and evolve, and it is unlikely to get less complex any time soon. You are now a little better prepared to understand the impact of future changes within the legal landscape, and hopefully you have come away with a better understanding of employee content monitoring.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

10. References

American Management Association (AMA)/ePolicy Institute Research. (2007). 2007 Electronic Monitoring & Surveillance Survey. Website: http://www.amanet.org/research/pdfs/electronic-monitoring-surveillance-survey08.pdf

BBBOnLine, Inc and the Council of Better Business Bureaus, Inc. (n.d.) A Review of Federal and State Privacy Laws. Retrieved October 15, 2008. Website: http://www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf

California Senate Bill No. 1841. (April 19, 2004). Retrieved on February 8, 2009 from Website: http://www.steptoe.com/publications/315c.pdf

Candris, L.A.. (2007). Manager No-No's. Retrieved on 10/22/2008 from Website: http://www.financial-planning.com/news/manager-no-nos-528375-1.html

CFAA (n.d.). Retrieved February 13, 2009, from Wikipedia: http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

Department of Justice Office of Legal Education. (n.d.). Prosecuting Computer Crimes. Retrieved November 21, 2008, Website: http://www.usdoj.gov/criminal/cybercrime/ccmanual/ccmanual.pdf

Electronic Communications Privacy Act. (n.d.). Retrieved November 21, 2008, from Wikipedia: http://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act

Electronic Communications Privacy Act of 1986 § 201, 18 U.S.C. § 2701 (1986)

Gordon, Philip. (2007). Who Said Employees Have No Right To Privacy In Their Corporate E-Mail And Internet Access?. Retrieved on 10/31/2008 from Website: http://privacyblog.littler.com/2007/07/articles/electronic-monitoring/who-said-employees-have-no-right-to-privacy-in-their-corporate-email-and-internet-access/

Heydary, Javad. (2005). Companies Step Up Electronic Monitoring of Employees. E-Commerce Times, July 2005. Retrieved on 11/55/2008 from Website: http://www.ecommercetimes.com/story/44850.html

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Katz v. United States. (n.d.). Retrieved November 21, 2008, from Wikipedia: http://en.wikipedia.org/wiki/Katz_v._United_States

Monnat, D.E., & Ethen A.L. (2004). A Primer on the Federal Wiretap Act and Its Fourth Amendment Framework. Journal of the Kansas Lawyers Association, March 2004 Issue, p.12 – p.15

National Workrights Institute. (n.d.). Privacy Under Siege: Electronic Monitoring in the Workplace. Retrieved October 15, 2008. Website: http://www.labortech.net/pdf/workplaceprivacytestdoc.pdf

Olmstead v. United States (n.d.). Retrieved February 13, 2009, from Wikipedia: http://en.wikipedia.org/wiki/Olmstead_v._United_States

Provos N., Mavrommatis P., Rajab M.A, & Monrose F. (2008). All Your iFRAMEs Point to Us. Google Technical Report.

Treglia, Stephen. (2008)., Employee Computer Misconduct Laws [PowerPoint slides]. Retrieved on Website: www.cscic.state.ny.us/ security/conferences/security/2008/info/Day%201/ F1-Treglia%20Employee%20Computer%20Law.PPT

United States v. Simons. (n.d.). Retrieved February 12, 2009, from Website: http://www.cybertelecom.org/SECURITY/privacy.htm

United States v. Councilman. (n.d.). Retrieved February 12, 2009, from Website: http://epic.org/privacy/councilman

U.S. Department of Labor. (2008). Fact Sheet #36: Employee Polygraph Protection Act of 1988. Retrieved on 02/05/2009 from Website: http://www.dol.gov/esa/whd/regs/compliance/whdfs36.pdf

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Cyber Defence Canberra 2018	OnlineAU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced