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

Acceptable Use Policies and Workplace Privacy: Legal and Ethical Considerations

© SANS Institute 2004, Author retains full rights.

GIAC Security Essentials Certification (GSEC)
Practical Assignment – Option 1
Version 1.4b

Patrick Dubicki
Submitted 11/27/2003

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

Abstract

The role of the Information Security Professional encompasses many responsibilities within an organization. Depending on the organization and its structure, this person will normally be responsible for the audit of security policies and investigation into potential internal abuses. The audit process or investigation could involve areas that may encroach on the personal privacy of the employee. Included in this may be the review of an individual's e-mail account.

Company acceptable use policies, security awareness, legal concerns and ethical considerations influence an investigation involving an individual's e-mail account. The intent of this paper is to look at the current corporate environment in which an individual's right to privacy is often an issue in relation to corporate policy. This paper will address the development of corporate policies relating to acceptable system use and what, if any, expectations of individual privacy are involved. Recent legal discussions, government regulations and ethical considerations, which may affect this process, have been reviewed.

Introduction

The 2003 CSI/FBI Computer Crime and Security Survey stated that "theft of proprietary information caused the greatest financial loss ($70,195,900 was lost, with the average reported loss being approximately $2.7 million)." With these types of losses, it is quite likely that much of this information may be finding it is way out of the company from individuals within the company. Not only is there the risk of lost, but liability issues may arise due to the improper use of resources provided. In the CSI/FBI report, 80% of the respondents reported insider abuse of Internet access. What can companies do to provide employees with the systems and information that they are required to have in order to fulfill their job responsibilities and at the same time control and mitigate the risks involved.

The major steps required to mitigate these risks are policy, awareness, monitoring, audit and investigation. Implementation of an acceptable use policy and an effective security awareness program are the first levels of mitigation. Employees cannot adhere to rules and regulations if there are not clearly defined and disseminated throughout the company. Once in place, the adherence to and effectiveness of these policies can be reviewed by monitoring usage, auditing and if necessary, investigation of possible abuse. The process of monitoring and investigation brings up the question of legal propriety and ethical issues. It is important that the security professional understand the various aspects of these issues in order to understand the potential risks involved. It is important to work with the appropriate groups, such as human resources and legal, when advising corporate management on policy. Any expectations of privacy must be clearly documented and made known to all employees. This is necessary in order to avoid risks when an audit or investigation is to take place.

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

Policy and Awareness

To address the issue of workplace privacy a company must establish policies that define the rights or privileges that employees have. Merriam-Webster's dictionary defines privacy as "a: the quality or state of being apart from company or observation b: freedom from unauthorized intrusion". The first step in the process is to define and establish a set of policies to address the needs and the expectations of the company. Included in these policies would be a definition of what is appropriate use of system resources and what is allowable and "authorized" intrusion. Some of the main points that an acceptable use policy would contain are:

1. The business reason for the policy
2. The scope of the policy, i.e. what areas are covered by this policy
3. Document any expectation of privacy that may exist – there should not be any on company provided resources
4. Document enforcement policy and disciplinary actions
5. A statement that the use of company resources is a consent to adhere to the policy.

In creating this policy, it is important that all areas of concern should be addressed in explicit terms. CSO magazine reports that 80 percent of companies have an acceptable use policy. Some companies establish policies that do allow some personal use of the Internet and corporate e-mail systems. These exceptions can lead to problems for the company. This allowable use portion of the statement is open to interpretation by the employees under which they may assume that they have some rights to privacy. Therefore, in the development of the acceptable use policy, it is best to prohibit any personal use of corporate resources regardless of what they are. In this way, there are no gray areas open to interpretation.

The documentation of any monitoring or inspection that will be done can address the needs of an audit or other similar investigation. A company policy may state that, "The company will inspect, and monitor the use of, information systems, including computers, voice mail, telephone logs, e-mail and Internet access and use to assure full compliance with policies, procedures and other guidelines defined by the company. Inspection and monitoring of these systems are conducted at the company's discretion." A policy statement such as this addresses the various resources and, by stating up front that they “will inspect and monitor”, eliminates the potential misinterpretation by an employee. This is not to say that each e-mail message that is being sent through the company system is being read by someone other than the person it is intended for. The language is meant to eliminate any doubt as to whether or not they can be looked at.

Once these policies have been established, they must be disseminated in a manner so that all employees are aware of them and agree to the conditions. The policies would be provided to new hires as part of their orientation program. An overall company security awareness program would be used to reinforce this and other security policies. The policies must be easily accessible to all employees at any time and stressed in

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

company publications, on the corporate Intranet and each time a user logs into his or her system. It should be clear that these policies apply to all individuals, employees, consultants, contractors and vendors. Anyone who is provided resources by the company must adhere to the policy.

There are other issues, which must be considered in the development of the policy. Many of the employees may see this as an intrusion of their privacy and will resent the implications that go along with this. The Institute for the Management of Information System (IMIS), an organization based in the U.K., addressed this concern. In an article on workplace surveillance they state that in June of 1997, "the European Court of Human Rights ruled that workers have a 'reasonable expectation' of privacy in making and receiving telephone calls at work."(Rogerson & Fairweather, 1998). The IMIS assumption was that this would apply to other means of communication, including e-mail. In an article in the New York Times, Judge James M. Rosenbaum, a chief judge of the United States District Court for the District of Minnesota, stated that he had reservations about an employee not having any rights in a search through their computer systems electronic files. Judge Rosenbaum was quoted as writing:

> "Most employees are not governmental entities, so constitutional search and seizure issues are not directly implicated. But just as an employee does not surrender all privacy rights on "the company's premises, so they should not be automatically surrendered on the company's computers."(Privacy Digest, 2001).

Recent surveys suggest that seventy-five percent of medium to large corporations are doing some type of monitoring. With three-quarters of U.S. firms performing monitoring, it could be argued that this is an acceptable practice and that there should not be an expectation of privacy in the workplace.

To effectively implement these policies, it is important that all employees must acknowledge and consent to these policies. Having a message that requires agreement to acceptable use policies before connecting to company resources can help to accomplish this. The message should let everyone know that all work performed with the computer system should be for business purposes only, and that any transmissions will be monitored and to continue will mean acceptance of this policy.

In a recent court case, *TBG Insurance Services Corporation v. the Superior Court of Los Angeles,* an employer provided an office and a home computer for an employee. The employee had signed an agreement that the employer could monitor the use of the computers. The company had discovered the employee had used the home computer to view pornographic sites and dismissed the employee. The former employee then sued for wrongful termination. The employee then refused to deliver the home computer during the investigation, believing that he had a right to privacy in his home use of the computer under the California Constitution. The court disagreed because the employee was made aware of the intention of the company to monitor computer usage. This eliminated any expectation of privacy. In addition, by using the computer after being

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

informed of the monitoring, the employee implied consent to the monitoring of his use (Kennedy & Stella, 2003).

While drafting a new policy, existing business concern should be taken into consideration. Among these would be the FTC Data Safeguarding rules and the potential liability of the company. The Data Safeguarding rules are intended to protect the privacy of customer information and to ensure that this information is not released outside of an organization. This can happen when an e-mail message which is meant to be sent internally or to specific individuals, is inadvertently sent to many others outside of the organization.

This was the case in an e-mail message intended for customers, which was sent out by a major drug manufacturer. They provided an e-mail notice to users of a prescription drug with information about the drug on a monthly basis. They had decided to stop this practice so an e-mail was sent out to those receiving the monthly notices. In sending the notice they, by mistake, included everyone's e-mail address in the "To:" field so that someone who received the message could see everyone else's e-mail address. Normally a message like this would be sent so that you would only see your own e-mail address. Now anyone who received the message could identify several hundred other potential users of the drug. The Federal Trade Commission found the company at fault for the release of the information and fined them $160,000 although it was considered an accident. Since the company had stated that they had promised to safeguard their customer's data, the FTC found them at fault for what they deemed to be an unfair or deceptive act (Kiefer & Sabaat, 2002). The FTC has the potential to shut down any e-commerce operation if it sees this as a risk because the company fails to protect its customer's information.

Business risks need to be taken into account when developing policies. Failure to take reasonable precautions to protect information such as customer data or financial projections could result in serious repercussions to the company. These policies must be developed with an understanding of business operations. Policies should not be developed in a vacuum, but with the understanding and cooperation of those affected.

Monitoring

Once the policies have been established, it is now important to implement a monitoring process to validate adherence and to flag violations. The CSI/FBI report stated that the total annual losses attributed to insider abuse of the Internet total more than $50 Million for 2002. The monitoring process should include those areas identified in the policy document. Monitoring Internet use can help identify those individuals who are visiting unauthorized sites, using large amounts of bandwidth or spending more time on the Web than on their jobs. Monitoring e-mail messages that are coming from outside the company can help to protect information systems from computer viruses, worms, or an overload of Spam mail. It is also a liability protection for the company to ensure that e-mails sent through the company do not contain any questionable or

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

objectionable material. The use of software that can monitor and record transmissions would be used to provide some of these protections.

Monitoring e-mail that stays within the company is important as well. Failure to intervene when e-mail messages may contain evidence of harassment or discrimination could leave a company open to lawsuits. The attempts to monitor these systems though have been impacted by government legislation. In 1986, Congress enacted the Electronic Communications and Privacy Act, which limits an employer's monitoring ability. The ECPA imposes both civil and criminal liability to anyone who either intercepts or plans to intercept electronic communication. The ECPA has three stipulations that employers must follow to be exempt from liability. First they must have prior consent, second, the interception must be for business use and third, you must be the service provider (Ziulkowski, 2002). The company policy should clearly define these items. The policy should let all employees know that they should not expect privacy when using company equipment and systems and the importance of not transmitting confidential information, especially outside the organization.

This policy and the monitoring of e-mail and other systems are primarily to protect customer data and the company. An important way to do this is to be sure that an employee knows the risk that the company is exposed to when electronic mail and data ends up in the wrong hands. It is vital that a document classification system be developed so that the employees will know what type of data they are working with. Information that is considered secret or confidential should be clearly identified so that there is no question as to how it should be handled. This can go a long way to gaining acceptance to the policy.

The company must also avoid any practice that may look as though they are targeting any individual or group. The monitoring should be performed across all areas of the company without regard to position. This raises the question of who should be doing the monitoring. Due to the nature of information that may be available, financial data, personnel issues, etc., this responsibility should be limited to specific individuals within the security organization. Any requests to view this information should be made through this group and meet strict guidelines before being released.

During the course of a security investigation or audit, a request can be made for information of those in the organization that may be part of, or the target of, the investigation. As part of this investigation, a review of e-mail messages that had been exchanged relating to what is being investigated will be done. In this instance, the original author of the message probably did not think that others outside their intended audience would have read these e-mail messages. Reviewing e-mail during the course of an investigation may be standard in many companies; this is similar to requesting copies of paper documents or other types of evidence.

Normally, when an audit or investigation is first initiated, a request is made that no paper documents are shredded and that no electronic information is deleted. Having the implied consent of the employees through their acceptance of the usage policy

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

minimizes some of the concerns with reviewing e-mail. It may not be pacify the individual but it should not be unexpected. More often, the concern is what else may be read that is not part of the intent of the investigation. Because of this, it is important that the scope of the investigation be defined and adhered to.

Legal Considerations

Most often, the issue of privacy arises during an investigation questioning whether this is a violation of the individual's Fourth Amendment rights. The Fourth Amendment protects an individual from unreasonable search and seizures. The U.S. Department of Justice provides extensive documentation relating to the gathering of electronic information in "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations". The document states that, "Warrantless workplace searches by private employers rarely violate the Fourth Amendment." It goes on to say that "In general, government employees who are notified that their employer has retained rights to access or inspect information stored on the employer's computers have no reasonable expectation of privacy in the information stored there."

The courts have approved of companies monitoring and reading e-mail in several cases. In *Smyth v. the Pillsbury Co.*, although the company had said it would not intercept e-mail or terminate employees because of it, the court ruled that no employee has a reasonable expectation of privacy when using company e-mail systems. Three separate cases were rejected in California dealing with wrongful termination in which employees objected to the monitoring and reading of their e-mail (Cotton 2000)

Although the court ruled with the one company even when their policy was not strict in regulating e-mail monitoring, it is still a better practice not to established policies that can be open for interpretation. When conducting an investigation, it is easier to accomplish required tasks if policies and procedures exist which can be given to employees should questions of privacy come up.

Two recent federal documents may influence this area of investigation, the National Strategy to Secure Cyberspace and the USA PATRIOT Act. Each of these documents is intended to address the growing concerns of terrorism, both foreign and domestic.

In the National Strategy to Secure Cyberspace, the importance of the public-private partnership is mentioned in several areas. In the plan it states that "The federal government promotes the creation of, and participation in, public-private partnerships to raise awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information and plan recovery operations." Further on the plan discusses privacy and states that "Consumers and operators must have confidence their voluntarily shared, nonpublic information will be handled accurately, confidentially and reliably."

The USA PATRIOT Act has entries, which relate to the disclosure of electronic communications. Section 212 of Title II covers "Emergency Disclosure of Electronic

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

Communications to Protect Life and Limb" which includes both the voluntary and required disclosure of customer communications or records. These disclosures identify the need for a "provider of electronic communication services or remote computing services" to inform the government of customer communications if there is a threat to life and limb.

This may require that private businesses monitor their e-mail systems for what could be considered a risk to national security (terrorist or anti-government type messages). In light of this, Thomas Jefferson stated "Let the eye of vigilance never be closed." Could this be a modern interpretation of that statement? Have we gone from monitoring e-mail for the protection of the customer and the company, to monitoring it for the protection of our nation? With the events of 9/ll, all transmissions of information are now under a watchful eye. Could this be a greater risk to personal privacy in the workplace? Who will determine what mail is a risk to our security? Currently, all that is seen and read within a company normally stays within the company. In the future, companies could be asked to turn this information over to the government. Do new policies have to take into account anti-terrorist policies? This could become a greater privacy concern for the employee. They could look to the company for protection from government investigations. It could also be an added risks for the company if they should release information that turns into false accusations.

It is probable that this will influence our roles in security. To ensure that we comply with new laws and regulations requires vigilance on our part to be aware of changes and what impact they have. Once we understand these changes, we will need to proactively review and change any policies as needed and provide this information to the rest of the organization. An effective method for this process is to develop a cross operational group with members of the legal department, human resources, physical security, records management and operations to discuss overall security concerns and any new issues that may arise.

Ethical Considerations

Tracking employees is not new to the electronic age; it just may be easier. Milton Hershey, in the early 1900's, would view the homes of employees to see how they were being maintained and had Hershey Park watched to see who was throwing trash on the lawns (Hoffman, Hartman, Rowe 2003). With most of today's transactions being recorded electronically, the risk for abuse by those with access to this information has increased greatly. For this reason, those in the security profession must adhere to a strict code of ethics.

Ethical considerations when conducting an audit or investigation must be taken into account. As a member of a professional organization, there is normally a code of ethics to follow and this code will often address the handling of confidential information. In the Code of Ethics for the Institute of Internal Auditors, it states that "Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional

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

obligation to do so." During the review of an e-mail account it is very likely, that personal information not related to the investigation could be viewed. As a security professional, it is our responsibility to realize this and to handle the information properly. In this way, the information is protected so that it goes no further than those who need to know.

Is it likely that during an investigation that the thought of invading someone else's privacy while reviewing their information could come up. With the recent scandals that have occurred in large corporations, it is important that all material be reviewed so that nothing is overlooked. This can lead to discovering problems within an organization and it is the only means to be sure that you have the whole picture. Missing any relevant data could lead to major problems for the company or the wrong individual may be held accountable for something they were not responsible for.

Conclusion

Individual rights and privacy are at the forefront of many issues today. The privacy of the employee within any organization must be respected, but the employee must understand the risks to the business for failure to properly use company resources. When in a corporate environment, employees may question what is being done in the name of security. With the potential for litigation, it is imperative that expectations of privacy are documented and known by all employees. Employees must know that systems use will be monitored and that there are serious repercussions if they are abused.

A Brief but Direct Sample Policy

It is the intent of the company to conduct business that meets all legal and regulatory requirements and to adhere to high ethical standards. The company is here for the benefit of its customers, its employees and its investors. In order to effectively conduct business the following rules must be adhered to by all users of corporate systems:

1. That all resources provided by the company including, but not limited to, computers, PDAs, e-mail, voicemail, company telephones, and Internet use, are to be used exclusively for business purposes.

2. All information deemed as secret or confidential or other proprietary information should not be released outside of the company without proper authorization.

In order to verify that these rules are enforced, the above named systems will be monitored and reviewed for compliance. The frequency and depth of these reviews are at the discretion of the company.

Failure to comply with this policy will result in disciplinary action up to and including termination and legal recourse if necessary.

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

By use of these systems, you are accepting these requirements and accept potential consequences for abuse of these systems.

© SANS Institute 2004, Author retains full rights.

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

References

Carson, C. & Fisher, D. (2002). Bush's Cyber-Security Plan Targets E-Mail. Retrieved August 23,2002 from eWeek Website http://www.eweek.com/article2/0,4149,481225,00.asp

Cotton, C. (2000) "Electronic Mail In The Workplace: Employer Monitoring vs. Employee Privacy" http://articles.corporate.findlaw.com/articles/file/00051/005814/title/Subject/topic/Constitutional%20Law_Privacy%20Rights/filename/constitutionallaw_1_91

Hoffman, W. M., Hartman, L., Rowe, M. (2003) "You've Got Mail . . . And the Boss Knows:" Business and Society Review, http://www.blackwellpublishing.com/images/Journal_Samples/BASR0045-3609~108~3~166/166.pdf

Institute of Internal Auditors Code of Ethics (2003) http://www.theiia.org/iia/index.cfm?doc_id=604

Kendall, Sandy (2003) "What's an Acceptable Acceptable-Use Policy?" http://www.csoonline.com/talkback/012703.html

Kennedy, C., & Stella, W., (2003) Big ~~Brother~~ Employer May Be Watching: Monitoring Employees' Online Communications In The Workplace. http://library.lp.findlaw.com/articles/file/00070/008922/title/subject/topic/computers%20%20technology%20law_internet%20privacy/filename/computerstechnologylaw_1_80

Kiefer, K. & Sabett R. (2002) Am I Liable?, CISO Magazine – Supplement to Information Security Magazine, 22-26.

Merriam Webster Online (2003) http://www.m-w.com/home.htm

Porter, K., Wilson, D. and Scheib, J. (2002) Work station or purgatory? Steps Toward a Company Policy and Using the Net, Business Law Today, July/August, 59-62.

Privacy Digest (2001) New York Times - Reconsidering the Privacy of Office Computers. http://www.privacydigest.com/2001/07/28

Rogerson, S. & Fairweather, B. (1998). Surveillance in the workplace. The Institute for the Management of Information System http://www.ccsr.cse.dmu.ac.uk/resources/general/ethicol/Ecv8no3.html

Schneier, B. (2000) Secrets & Lies Digital Security in a Networked World. New York: WileyComputer Publishing.

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

"The National Strategy to Secure Cyberspace"
http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

United States Department of Justice (July 2002) "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"
http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf

Ziulkowski, J. (2002) Employer Beware, What You Don't Know Can Hurt You: E-Mail Monitoring and Privacy Issues in the Private Sector Workplace. The Michigan Business Law Journal, Summer, 22-24.

© SANS Institute 2004, Author retains full rights

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