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 the Law: Governing Investigations

GSEC Version 1.4b Option 1

Todd Storey
September 22, 2002

© SANS Institute 2001 - 2002, Author retains full rights.

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

Abstract

The results of numerous surveys of information security professionals and statistics from law enforcement lead us to believe it would be wise to adopt a stance of preparation for "when" an incident occurs as opposed to operating under the premise that you will react "if" one occurs. A well detailed and rehearsed incident response plan is important to enable a rapid re-establishment of operations and to collect evidence should identification and prosecution of the perpetrator(s) be desired.

An equally important element in the preparation for such an occurrence is the implementation of a well-planned Acceptable Use Policy, or AUP. The contents (or lack thereof) of the AUP will govern what type of evidence may be collected during an investigation and how. This is even more pronounced when the focus of an investigation is a company insider. If the desired result of the investigation is disciplinary action or prosecution, a poorly planned AUP will not only hamper or limit the investigation, but may even expose the investigator himself to criminal or civil liabilities.

This paper will examine the legal issues that define the scope of an investigation under United States law. Emphasis is placed on cases in a corporate environment where the suspects are company insiders. The role of an AUP in such a setting will be presented along with important considerations in its development.

Please note: This paper is intended to illustrate the legal issues guiding a corporate investigation by providing a basic portrayal of relevant United States laws, whose interpretation can be very complex. As such, this information is not intended to convey legal advice.

Acquisition of Evidence

A key element to any investigation whether performed privately or by a government agency is the acquisition of evidence. When investigating an incident on a corporate network, it may be desirable to perform any or all of the following procedures:

- Search an employee's machine for evidence.
- Request information from ISP's or other third parties.
- Perform network surveillance.

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

Whether or not you as a corporate investigator can *legally* perform any of these tasks on your network is determined to a large degree by your Acceptable Use Policy.

To illustrate this point, it is first necessary to take a closer look at how investigations requiring these intrusive measures are performed by government agencies (whose actions are not governed by AUPs), and the legal impediments to performing them.

Searching a Suspect's Computer for Evidence

A fundamental concept limiting investigations by government agents in the United States is that of "a reasonable expectation of privacy" of its citizens. This right is granted in the Fourth Amendment to the Constitution and is central to the approval of search warrants, which must be obtained prior to searches of computer equipment (with certain exceptions).

The Fourth Amendment 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.

"Probable cause" is defined as "where known facts and circumstances, of a reasonably trustworthy nature, are sufficient to justify a man of reasonable caution or prudence in the belief that a crime has been or is being committed." Draper v. U.S., 1959.(1)

In other words, it is necessary for a government agent to present a judge with an affidavit providing sufficient information to convince him of probable cause. One can see the logistical problems this can present in cases where hundreds or thousands of computers reside on a corporate network and time is precious.

In addition to the headaches involved with this procedure, it may not even be possible for an agent to obtain a search warrant because they are only issued as part of a criminal investigation. Many offences can be considered inappropriate or immoral in nature but are not necessarily criminal.

The Fourth Amendment also requires that all warrants will be issued "particularly describing the place to be searched, and the persons or things to be seized". Therefore in order to pass a constitutional challenge, a warrant (1) must provide sufficiently specific information to guide the officer's judgment in what to seize, and (2) the warrant's breadth must be sufficiently narrow to avoid seizure of

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

purely unrelated items. This makes it difficult to meet the constraints of the Fourth Amendment as computers store enormous amounts of information and files names are not necessarily indicative of their contents. Some courts have invalidated warrants that were deemed to lack sufficient particularity or limitation in scope.

Requesting Information from Third Parties

The Electronic Communications Privacy Act (ECPA) of 1986 was adopted to address privacy issues that arose through the development and increasing use of new modes of electronic communication. It attempts to define what constitutes an invasion of privacy when electronic surveillance is used. The ECPA extends privacy protection to cellular telephones, pagers, email, computer transmissions and private communications carriers.

If access to the network under investigation was gained from outside of the organization, an investigator would benefit greatly by being able to obtain logging data from sites where the attack was launched as well as information from Internet Service Providers.

There are many requests that a government investigator may ask of an ISP. A summary of these items and the procedures required to obtain them are defined under Section 2703 of the ECPA:

- Basic subscriber information such as name, address, local and long distance records, subscriber identification numbers, duration and types of services utilized must be obtained through the issuance of a subpoena as defined in 18 U.S.C. § 2703(c)(1)(C).

- Opened emails can also be obtained if conditions requiring notice to the subscriber have been met under 18 U.S.C. § 2703(b)(1)(B). This action also requires the issuance of a subpoena.

- Account logs and transactional records must be obtained through a court order under 18 U.S.C. § 2703(d) which requires the agent to present "articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation"

As can be seen, the ECPA represents another significant barrier to investigations by law enforcement agents, this time in controlling the disclosure of information from electronic communications providers.

Performing Network Surveillance

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

Obtaining permission to perform network surveillance can be challenging and complex from a legal standpoint. Government agents are likely required to obtain a Title III nonconsensual wiretap which permits the interception of electronic communications.

The "wiretap statute" or Title III (18 U.S.C. § 2511) makes it illegal for anyone to intercept wire, oral or written communications while they are being transmitted. In order to obtain a Title III nonconsensual wiretap, one of the following statutory exceptions must apply:

1. **Interception authorized by a 2518 court order** - A Title III court order is authorized by a District Court or Court of Appeals judge and permits law enforcement to intercept communications for up to 30 days. The application must show probable cause to believe that interception will reveal evidence of a felony offense.

2. **The 'consent' exception** - This exception authorizes interception when one of the parties has given consent to the interception. One of the parties can be a system administrator or a law enforcement official.

3. **The 'provider' exception** – Communications service providers can intercept and disclose communications in order to protect their rights or property. The intercepted information can then be passed on to law enforcement. This exception by no means applies to law enforcement officials, who are in no way permitted to initiate, influence or participate the process.

4. **The 'extension telephone' exception** – This exception was originally intended to permit businesses to monitor the conduct of employees when speaking with customers. This makes the monitoring of employee communication legal when conducted for legitimate work-related reasons. This exception does not apply to law enforcement agents, some of whom in the past have intercepted telephone conversations on the theory that it was in the ordinary course of his duties.

5. **The 'inadvertently obtained criminal evidence' exception** – This exception permit a public electronic communications provider to disclose to contents of a communication to law enforcement if the communication appears to be relevant to the commission of a crime. This exception remains relatively unapplied to cases involving communication with computers via internet service providers.

6. **The 'accessible to the public' exception** – This permits anyone to intercept a communication made through a system that is readily accessible to the general public. This would apply to the interception of a

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

communication that has been placed on a public bulletin board system or newsgroup.

As will be seen later on, the most applicable of the six exceptions to the system administrator and the corporate investigator is the second exception, or the 'consent' exception.

Once again law enforcement is faced with highly restrictive and time consuming requirements to perform investigative measures, this time when performing network surveillance.

As can be seen in the preceding section, when a law enforcement official wants to access a computer to search its contents, retrieve information from third parties or perform network surveillance, there are a strict set of conditions that must be met in order to preserve the rights of those being investigated. Failure to preserve these rights can at best result in the suppression of evidence in court, and at worst expose the investigator to criminal or civil liabilities.

The most important concept governing these investigative steps is the right of the suspect to "a reasonable expectation of privacy" which exists to protect citizens from unreasonable search and seizure.

If evidence collected is eventually presented in a court of law, the defense will commonly challenge its admissibility based on the concept that the defendant's right to a reasonable expectation of privacy was violated when the evidence was collected. It is up to the judge at that point to determine whether the individual's subjective expectation of privacy is one that society would be willing to agree with, and either admit or suppress the evidence.

A well planned Acceptable Use Policy in the workplace addresses this issue by clearly indicating to employees what activities will be monitored. The AUP will in effect define their expectation of privacy.

Developing an Acceptable Use Policy

The process of developing an AUP can be a sensitive one requiring a balancing of variables. On the one hand, management typically would like the freedom to access all employee communications if and when circumstances require it. On the other hand, employees feeling that they have relinquished all of their rights to privacy in the workplace can experience reduced morale.

In simple terms, an Acceptable Use Policy is a document that states how users or employees are permitted to use an organizations information systems. The following issues are a just a few of the topics most commonly addressed:

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

- Internet usage – internet connectivity is provided solely for the purposes of achieving the goals of the organization. Visits to unrelated sites such as investment bulletin boards or those containing adult content is prohibited.

- Unauthorized software installation – all software must be approved by the designated authority prior to installation.

- Illegal activities – equipment must not be used for activities which are in violation of the law.

- Authentication – userID and passwords are to be kept confidential.

- Proprietary or confidential information – no proprietary or confidential information can be sent to third parties.

- Violation of policy – employees who violate the terms of the AUP will be subject to disciplinary action or prosecution.

More importantly, from an investigative and incident response perspective, the inclusion of the following topics is of central importance:

- Ownership – all data created on the company's information systems is the property of the company.

- Monitoring – a specific individual(s) may monitor all equipment and traffic on the network to ensure proper operation and compliance with the other directives.

It is these final two areas that will define the degree of an employee's expectation of privacy. Here the company must balance its desire for full access to all communications with their employees' desire for privacy. When the AUP has been agreed to as a condition of employment, employees should have a clear understanding of the extent of the company's right to access their communications and therefore their expectation of privacy.

Employers should always consult their legal council when preparing their company's AUP to ensure it does not conflict with other company policies or laws.

Corporate Investigations

The clarification to employees of what activities can be monitored by the company can dramatically simplify the investigative process in a corporate setting.

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

As a result, corporate investigations are afforded much more freedom. Some of the benefits to a corporate investigation include:

- The investigation can proceed at a much faster pace.
- A corporate investigation can prevent knowledge of the attack from becoming public (the resulting damage to business from public knowledge of an insider security breach can easily exceed the damage from the attack itself).
- The company can guide or terminate the investigation as any number of internal conditions may require.
- Corporations can pursue cases in civil court where proof is based on a "preponderance of the evidence" as opposed to the more stringent requirement of "beyond a reasonable doubt" in criminal cases.
- With an appropriate AUP, many intrusive investigative measures can be implemented that would not be permitted by law enforcement or would require a difficult approval process.

In order to be ensured the investigative and evidentiary freedom afforded by an AUP, it must be in place prior to the incident which is being investigated. If one was not in place, the investigative measures undertaken and evidence presented in a court of law will be governed in a large degree by the tedious federal and state-level statutes that govern law enforcement agencies.

Investigations by government agencies can be inhibited or prevented by the slow processing or denial of the necessary permissions. The corporate investigator is able to perform these same tasks with comparatively few obstacles. Although the AUP and other company policies can greatly simplify these steps for the corporate investigator, some important precautions must still be taken. We can now return to the three intrusive investigative steps discussed earlier to see the different manner in which they are conducted in a corporate investigation under the guidance of an AUP.

Searching an Employee's Computer for Evidence

When a corporate investigator wants to search an employee's computer for evidence that may end up in a court of law, he will typically make an image of the suspect's hard drive using a commercially available product for windows environments or in the Unix environment use the dd (data dumper) utility. A forensic analysis can then be performed on a copy of the image. A search warrant would be required by law enforcement to perform this procedure, but a company AUP which clearly states that all data created on the company's information systems is the property of the company will permit this, and the

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

evidence would be likely to withstand any constitutional challenge by the defense.

An important consideration to be aware of when accessing employee email is that there is a difference between accessing a message that has been read and in residing in storage on an employee's machine and accessing unread messages. Without a proper policy to the contrary, accessing unread messages can be considered an interception of communications and would likely be in violation of the ECPA.

Requesting Information from Third Parties

System administrators or corporate investigators can typically obtain valuable information from third parties simply by calling and requesting it. This can include the services used by the account holder as well as transactional information. This ease of access is contrasted with law enforcement who must first prove the relevance of the information to a criminal investigation and obtain a court order.

Although the ease of obtaining this information cannot be attributed to the company policy at the site of the incident, the terms of the AUP of the third party can play an important role in the manner in which this information can be released. This type of disclosure is also permitted under the "provider exception" to the wiretap statute discussed earlier where the ISP is acting in the protection of its rights of property and proper operation of its services.

Performing Network Surveillance

The requirements of the federal wiretap statute can permit full content network surveillance by a corporate investigator under the second exception or the "consent exception". Obviously this implies that explicit written consent should be obtained if it is not clearly stated in the AUP. If it is questionable as to whether full content monitoring could be considered an invasion of privacy and obtaining written consent is not an option (as in cases where the suspect is a company insider where alerting him to your activities is not desirable), then a "pen/trap" is a less intrusive option that can prove quite useful. Pen/trap is short for a pen register and trap and trace, terms which were originally applied to the outgoing and incoming addressing information of monitored phone calls. When a pen/trap is applied in the setting of network surveillance, no actual packet contents are captured, only the network and transport layer header information. This is often a useful tool in locating the source of trouble on a network and at the same time preserving the privacy of employees.

The use of banners also prove beneficial to an investigation when deployed on corporate networks. Banners are warning messages that appear to users when they logon to the system. They will typically contain a warning message to the user that by logging on they are consenting to potential monitoring.

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

This is useful in cases where the investigation leads to the discovery of a security breach by an outsider or the establishment of a covert channel of communication between an insider and a party outside of the organization. In this case, company insiders may have consented to monitoring in the AUP, but now the outside party has also given consent by having read the banner message. This has been a problem in the past because even unlawful intruders could have an expectation of privacy. If a system is properly bannered, any evidence collected that is challenged in a court of law should stand if the investigator can prove the outsider saw the warning banner. Banners can also be used to provide supplementary protection to the terms of the AUP against invasion of privacy claims.

The following is an example of a warning banner from the CERT website (2):

```
This system is for the use of authorized users only.
Individuals using this computer system without authority, or in
excess of their authority, are subject to having all of their
activities on this system monitored and recorded by system
personnel.

In the course of monitoring individuals improperly using this
system, or in the course of system maintenance, the activities
of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring
and is advised that if such monitoring reveals possible evidence
of criminal activity, system personnel may provide the evidence
of such monitoring to law enforcement officials.
```

Staying up to Date

Is important for incident response teams and corporate investigators to be vigilant for any developments in the legal system that can affect the collection of evidence and its admissibility in a court of law.

One such recent development has been the passing by Congress of The Patriot Act in October of 2001. In addition to tougher new penalties for those convicted of computer crime, an important element of the act defines a “computer trespasser” and states that such trespassers have no rights to privacy under the ECPA. This can relieve some of the concern of investigators when presenting evidence where bannering systems were not in place.

The Patriot act also affects the investigative process by granting the right to law enforcement to assist in the monitoring of network traffic without a Title III wiretap. This can be permitted when certain conditions are met, one of which is obtaining permission from the owner of the equipment.

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

These developments to date remain somewhat untested, however changes of this significance are sure to continue in the years ahead.

Conclusion

Incident response teams and corporate investigators must not only be technically proficient in their field, but must also have a sound understanding of the laws governing the collection of evidence and workplace privacy issues. Equally important to their knowledge of the relevant federal and state-level statutes is ensuring that the Acceptable Use Policy of their organization provides the proper permissions to implement intrusive investigative measures. The terms of the AUP can provide the consent required for exemption to most laws governing employee monitoring in the United States. Most importantly, the AUP provides employees, management and investigators with protection by defining the activities permitted on the network by all parties.

© SANS Institute 2001 - 2002, Author retains full rights.

Resources:

United States Department of Justice. “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.” July, 2002. URL:http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm (September 21, 2002).

United States Department of Justice Computer Crime and Intellectual Property Section. “Privacy Issues in the High-Tech Context.” March 27, 2001. URL:http://www.usdoj.gov/criminal/cybercrime/privacy.html (September 22, 2002).

Electronic Frontier Foundation. “EFF Analysis of the Provisions of the USA Patriot Act.” October 13, 2001. URL:http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (September 20, 2002).

Rubinstein, Geoffrey. Jones Telecommunications & Multimedia Encyclopedia. “The Electronic Communications Privacy Act.” (1994). URL:http://www.digitalcentury.com/encyclo/update/ecpa.html (September 19, 2002).

United States Department of Justice Computer Crime and Intellectual Property Section. “Searching and Seizing Computers and Related Electronic Evidence Issues.” December 17, 2001. URL:http://www.usdoj.gov/criminal/cybercrime/searching.html#B1 (September 21, 2002).

Ferraro, Crystal. “Deconstruction from the Inside Out.” searchSecurity. June 25, 2001. URL:http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci750604,00.html (September 16, 2002).

Mandia, Kevin and Prosise, Chris. Incident Response. Berkeley: Osborne/McGraw-Hill, 2001

Patzakis, John. “EnCase Legal Journal, Second Edition.” March, 2002. URL:http://www.encase.com/support/downloads/LegalJournal.pdf (September 21, 2002)

Briney, Andy. “2001 Industry Survey.” infosecurity Magazine. October, 2001. URL:http://www.infosecuritymag.com/articles/ october01 (September 21, 2002).

Kruse, Warren G. and Heiser, Jay G. Computer Forensics: Incident Response Essentials. Indianapolis: Addison-Wesley, September 2001.

© SANS Institute 2001 - 2002, As part of GIAC practical repository. Author retains full rights.

Verton, Dan. “Insider Monitoring Seen as Next Wave in IT Security.” Computerworld. 2002.

URL:http://computerworld.com/softwaretopics/software/story/0,10801,58671,00 (September 17, 2002).

Andrews, Sarah. “Workplace Surveillance: Trends and Recommendations.” July 18, 2001. URL: http://www.epic.org/epic/staff/andrews/workplace_surveillance.htm (September 21, 2002).

U.S. Department of Energy. “J-043g: Creating Login Banners.” May 9, 2002. URL:http://ciac.llnl.gov/ciac/bulletins/j-043.shtml (September 15, 2002).

References:

(1) Strickland, Ralph. Refreshing Your Recollection of Past Judicial Decisions. 1994. URL:http://www.jus.state.nc.us/NCJA/legoct94.htm (September 19, 2002)

(2) Carnegie Mellon University. CERT® Advisory CA-1992-19 Keystroke Logging Banner. September 19, 1997. URL:http://www.cert.org/advisories/CA-1992-19.html (September 21, 2002).

© SANS Institute 2001 - 2002, Author retains full rights.