Steps to Secure a Law Enforcement Network

David Brown

David A. Brown
GSEC Practical Assignment Version 1.3
Steps to Secure a Law Enforcement Network
March 16, 2002

Summary

I work for a statewide law enforcement network. This network provides on-line access to records concerning wanted persons, stolen vehicles, criminal histories, and other data of importance to law enforcement and criminal justice agencies. The state system also provides access to the National Crime Information Center (NCIC), which is maintained by the Federal Bureau of Investigation. Local law enforcement and criminal justice agencies connect to the statewide network to obtain this data and to communicate with other agencies throughout the United States. These user agencies must meet federal and state security requirements to insure confidentiality and integrity of the data.

Part of my job is to provide assistance to user agencies in securing their networks that connect to us. Oftentimes these agencies are operating under tight budget constraints with limited manpower and resources. They frequently do not have staff that are technically trained and use outside vendors to install and maintain their systems. Agency administrators often ask me what I would recommend they do to start securing these systems. This paper attempts to answer that question by addressing several common issues such as training for system administrators, risk assessment, physical security, security policies, and proper system administration.

Training for System Administrators

It is important to appoint at least two people to be responsible for the administration of a computer network and related systems. Why not use one person to have total responsibility for this function? There are two reasons.

The first is redundancy. By using at least two people, there is a backup person that can do the job if something happens to the other person such as discipline, illness, or even death. Many agencies use officers for this function, and remember that law enforcement is not the safest profession! It also makes it easier to spread the responsibility across multiple work shifts. If a computer operator fails to login to the system properly and locks his account at three o'clock in the morning, the system administrator on duty can restore the account immediately instead of waiting for hours or days for the other system administrator to come back to work from time off.

The second reason is to provide a system of checks and balances. If only one person holds control over a system, who else is there to watch and make sure this person is not setting up unauthorized user accounts, stealing data, or just failing to perform a system update or backup?

Once the people are appointed as system administrators, they need to be trained to do the job. There are several resources that provide training in computer security and

network administration. Some excellent providers of this training include, but are not limited to the following. Their web site addresses are provided for further reference:

Table 1

SANS Institute	http://www.sans.org
Computer Security Institute	http://www.gocsi.com
Global Knowledge	http://www.globalknowledge.com
MIS Training Institute	http://www.misti.com
Cisco Networking Academy	http://www.cisco.com/warp/public/779/edu/academy/overview/curriculum/

Many of these programs are short, weeklong classes that offer intense study in a particular subject area. Some of the providers also offer online training so that employees do not have to miss work or incur travel expenses. I have attended the Cisco Networking Academy, and I have found the instruction to be thorough. Their coursework is spread out over several weeks to several months depending on the program taken. The curriculum can be accessed from home or work and then time is spent in a lab each week to provide hands on training. SANS offers several different courses, but two in particular that may prove beneficial to agencies are the Security Essentials course, and the Information Security Officer course. The Information Security Officer program provides basic level information on computer security and network fundamentals. Security Essentials builds on this by providing a more in depth look at computer security and gets the student acquainted with Windows and Unix security. Both of these programs can be taken at a SANS Conference, and the Security Essentials course can be taken online. Each will involve several weeks of study at a minimum. Once completed, the student can pursue certification in either of these areas. Visit the SANS website for more information.

If these programs are not within reach, there are other resources that can provide low cost training. Local community colleges and joint vocational schools offer classes on networking, operating systems, and other computer training, which provide a foundation of learning to build upon. Some of these classes are only a few hundred dollars compared to thousands of dollars charged by private training firms. If even this is outside the capabilities of the agency budget, books can be purchased or loaned from the local library and on duty time can be provided so that the employees have time to study them.

There are other sources of training that are free. The National Cybercrime Training Partnership website states, "The National Cybercrime Training Partnership

(NCTP) currently sponsors training in Basic and Advanced Data Recovery and Analysis, through the National White Collar Crime Center (NW3C), Computer Crime Section."[1] Training is free for certain members of law enforcement and criminal justice agencies. These courses will teach system administrators how to obtain forensic evidence from computer systems, which can be used when agency employees violate security policies and criminal laws while on the job.

Several organizations exist that allow agency personnel to communicate with other system and security administrators and some offer various seminars at little or no cost. One such organization is InfraGard. Their national website states their mission:

> InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures.[2]

Membership in this organization is free in most chapters. Meetings are usually held on at least a monthly basis and cover a variety of topics. A list of chapters and a membership application are available on the national InfraGard website.

Another organization that provides for information sharing and training is ISSA®. According to their website, "The Information Systems Security Association (ISSA)® is a not-for-profit international organization of information security professionals and practitioners. It provides education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members."[3] There is a slight annual membership fee to belong to this organization. A membership application is also available on their website.

There are also free publications available to system administrators. One example is Information Security magazine, which is published monthly by TruSecure Corporation. It covers a variety of topics, and they annually publish a buyers' guide. This is an excellent resource to learn about security practices and new technology.

Risk Assessment

Once it is established who is responsible for the administration of the system and they have been provided with training to do the job, the agency should develop a plan to secure the computer network.

The first thing to do in developing such a plan is to perform a risk assessment. You cannot properly protect your network if you do not know what the threats are to it or its vulnerabilities. The Australian Computer Emergency Response Team website has several papers for reference on computer security topics. One such paper, entitled

"Improving Computer Security through Network Design" outlines several general steps to take in performing risk assessment. The first step is to:

> Identify the assets of the organisation that require protection. This may include physical items such as computer hardware, blank stationery, backup tapes; non-physical items such as data, software, network access; and other usually unrecognised important issues such as the organisation's reputation. (sic)[4]

Definitely, for law enforcement agencies, reputation will be important to consider. The citizens served by a criminal justice agency expect information about them to be kept confidential as much as is legally permitted. While government agencies must comply with public records laws, data obtained from NCIC and associated state law enforcement systems is usually not considered public record. Law enforcement agencies also keep confidential information on informants, investigations, floor plans of businesses, emergency plans, and various other records. Security incidents resulting in the theft of this data or system compromise will significantly scar an agency's public reputation if an investigation determines that they did not take due care to enforce proper security measures. Furthermore, the consequences can be much more serious. A denial of service attack on a police department's network may affect critical systems such as computer aided dispatching. The lives of officers, informants, and citizens can be put in immediate jeopardy should an incident of this magnitude occur, or if confidential information falls into the wrong hands.

The second step listed in the paper is to "Place a value on those assets. This will help determine the amount of security required later."[5] Certainly there is monetary value to replace a server, for example, but there are also other values to consider. Consideration for the number of man-hours to reprogram the server, and the amount of wages the people will be paid must be factored in. There is also the loss of time. If a police officer normally assigned to road patrol must spend extra hours doing system administration to restore a server, he cannot devote that time to his normal duties. There is also the inherent value a piece of equipment has to the operational status of the agency. If the server that runs the computer aided dispatch software goes down, this could have serious consequences to the ability of the agency to efficiently dispatch emergency calls. This would place a higher value on this asset than say an email server.

The third step listed is to "Determine what threats these assets may face. What are the attacks or problems that could adversely affect this asset (deliberate and accidental)?"[6] Threats could be physical such as fire, or could be other types such as attack via an Internet connection, a virus or worm contracted from electronic mail, etc.

The fourth step is to "Determine the types of vulnerabilities that could generate or cause this threat."[7] An example of vulnerability could be an open service (port) on a computer that would allow a denial of service attack. Another example would be personnel that are not trained in the proper dissemination of certain data, which could result in release of confidential information through social engineering.

The fifth step is to "Quantify the chance of a particular vulnerability actually occurring."[8] Consider for example, the possibility of a tornado occurring in your area. An article posted on a National Oceanic and Atmospheric Administration website states: "Tornado Alley includes parts of Texas, Oklahoma, Kansas, Nebraska, eastern Colorado and western Iowa, and is characterized by a high frequency of strong and violent tornadoes and a relatively consistent season from year to year."[9] If your agency were located in this area of the country, you would have a much greater potential to experience significant tornadoes than someone in another state such as Maine. There are additional statistics available from NOAA that provide a more definitive measure of the probability of this type of occurrence. Oftentimes, research will be required in order to acquire the information necessary to quantify the occurrence rate.

The technical director for the Australian Computer Emergency Response Team states, "By identifying the threats and their likelihood of occurring, and combining that with the value of the asset, we can quantify the loss we are likely to experience should that threat actually occur."[10] Once you have done these steps, you can prioritize what assets need protection the most, and what methods you can use to reduce the vulnerabilities and threats for that asset. Examples of actions to take might include the installation of a fire protection system, adding a firewall to limit network exposure to Internet attacks, or providing better training to computer operators so they better understand how to detect social engineering.

An excellent book that can guide you through the risk assessment process is entitled "Information Security Risk Analysis" by Thomas R. Peltier. This book provides different methods to perform risk analysis, sample forms to use during the risk analysis process, and even a sample report to use as a guide when you present your analysis to upper management.

Physical Security

One area that I often find lacking proper controls is physical security. This weakness should become evident in a proper risk assessment. While it may be one of the more basic areas of consideration, the obvious is often overlooked. An agency can design their network to have firewalls, authentication methods, intrusion detection, and a myriad of other protective measures, but this is all worthless if an unauthorized person can walk up to a wiring rack and rip the wires off the equipment or improperly shut down a server.

One would not suspect that physical security would be a problem in a law enforcement agency. Unfortunately, the agency's employees or vendors may be the very source of the problem. Employees may become discontent due to disciplinary actions taken against them or due to disagreements with management. I have learned of agency personnel deliberately destroying important documents because they faced layoff. Some vendors have installed unauthorized dial-up software without the agency's knowledge and created user accounts for system access. Others have made unauthorized changes to an agency's router. Each of these occurred because proper physical security measures were not taken.

Access to servers, wiring, and equipment must be limited. Wiring and network equipment such as routers, switches, and firewalls should be installed in locked cabinets or wiring closets with keys provided only to these administrators. Servers should also be located in locked rooms. Vendors and visitors should be accompanied at all times whenever they are in these areas, and a log kept of the time they arrive on site and the time when they depart. Prisoners who are trustees performing work within the agency should not be allowed access to these areas without supervision.

Consideration should also be given to materials leaving the agency. When printouts of sensitive information are to be thrown out, they should be shredded first to prevent someone searching through the trash and obtaining confidential data concerning a case or a person. When a backup tape is to be discarded, it should be passed through a strong magnetic field, burned, or melted to prevent the recovery of data. Even though a tape has been "erased" by the tape drive, it is still possible to recover data from it, so it is necessary to take this additional step.[11] When a computer hard drive is replaced, it should be electronically wiped of data before being discarded.

Security Policies

"A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."[12]

Many of the agencies I contact do not have computer security policies of their own. They may rely on those provided by the state law enforcement network or on that issued at the federal level. These policies only address general security requirements for connection to the state and federal networks and do not take into account local practices. It is important for each agency to establish their own set of policies to cover the following topics as applicable: anti-virus, dial-in connections, e-mail use, Internet use, network security, physical security, and hardware/software usage and installation. It is often very difficult to discipline employees for system misuse if there is no formal policy telling them not to do it.

Before an agency can establish security policies, the risk assessment must be completed. You need to know what areas of concern must be addressed by the policies. Supervisors and staff members having knowledge of the subject area should draft the policies. Once the draft document is prepared, it should be reviewed by legal council such as the city law director or prosecutor, and should always have the written approval of the agency administrator prior to distribution. Once approved, the policies must be distributed to all employees. Employees should read the policies and then sign off that they have read and understood them. The signature form should be kept for future reference in cases where disciplinary action is required. It is also good to require an annual review of these policies, again with sign off by the employee.[13] Employee training sessions dealing with these documents provide an additional documented effort to provide adequate knowledge of the policies to the system users.

A security policy must be realistic and attainable. For example, a good security policy would not require the installation of all security patches for an operating system, but rather only those patches that can be loaded without making the system unstable.

Some patches when loaded will crash a system due to compatibility problems and there is no work around solution to overcome it.

There can be no double standard in the enforcement of the security policies. They must apply to everyone and be enforced in a consistent manner. To be enforced, they must be enforceable.[14] A policy will not be effective if you have no way to monitor for violations of the policy. For example, if a policy is written that states employees may not access the Internet for personal reasons, you must have some method to monitor use. A common method is to employ content filter software, which looks for specific keywords when someone attempts to access a web site. If a keyword match is found, access is automatically denied by the software and recorded to a log that can later be reviewed.

There are excellent resources to assist agencies in developing security policies for the first time, or to help them build better policies than the ones they currently use. Thomas R. Peltier has written a book, Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management, which is published by Auerbach Publications. His book covers the topic from start to finish, giving many examples along the way. He also gives some information on ISO 17799, which is a recently released international standard on information security. A second resource is RFC 2196, which is titled Site Security Handbook. This document was published by the Internet Engineering Task Force (IETF) and was specifically written to provide guidelines on computer security policies and procedures. A SANS web page containing information on the SANS Security Policy Project is a third resource. It is located at http://www.sans.org/newlook/resources/policies/policies.htm and provides many sample policies for your use.

System Administration

Proper system administration is also a key factor in information system security. State and federal network security requirements mandated to user agencies require things such as firewalls, encryption, and strong authentication in some circumstances. These policies, however, do not often cover more fundamental measures that agencies often do not consider. During the course of many inspections, I have found several common problems that point to a lack of proper system and network administration. Some of these same areas area addressed in a document entitled "Generally Accepted System Security Principles" published by the International Information Security Foundation. This document provides general principles to follow, with accompanying examples. It is not intended to be a document detailing specific steps to secure a system.

One problem is that logging is not enabled on systems, whether they are servers, workstations, firewalls, or routers. "Information assets should be controlled and monitored with an accompanying audit log to report any modification, addition, or deletion to the information assets. These logs should report the user or process which performed the actions."[15] System administrators should examine logs frequently for signs of trouble. Many departments use Windows NT or 2000 operating systems because of their familiarity with the Windows environment. In these systems, the system administrator should activate security logs to capture login attempts such as someone

using a different user's account while the user is on leave. You can correlate these by comparing the login times to the personnel schedule. It can also capture file usage such as the deletion of system files by a person attempting to sabotage a system. System logs should be activated to indicate when problems are occurring with the computer that may need to be addressed. Firewall logs are also important to use because they provide an indication of how the device is performing. They also can be used for evidentiary purposes when intrusions are attempted or occur.[16] An excellent overview of firewall logging can be found at the Carnegie Mellon CERT® Coordination Center web site. The URL is: http://www.cert.org/security-improvement/practices/p059.html.

A second problem is poor account management. Oftentimes, a system administrator may set up user accounts and not check them again until an employee is hired. Accounts must be disabled when an employee resigns; otherwise a door has been left for them to enter the system without authorization. Accounts should be set to automatically lockout after a certain number of login attempts to prevent someone from using brute force methods to crack the password. Ideally, a system administrator should be required to reset a locked account, thus providing a method to notify this person that someone may be trying to access the system without authorization. Minimum password lengths should be enforced. The longer the password, the harder it is to crack. Many times I find passwords do not expire. It is important that password expirations be established so that if a user password is compromised, the intruder will not continue to have access long term. A regular review of user accounts should be conducted at least weekly to determine if an unauthorized account has been established. This could indicate an intruder has obtained administrator level access to the system. Separate accounts should also be set up for each vendor or contractor employee having any level of access to the system. These accounts should have limited access to only those rights and permissions necessary to do the work for which they have been hired. They should not be given complete administrator or super user rights if at all possible.

Another problem is the lack of anti-virus protection on workstations and servers. Anti-virus software exists to protect these devices from the introduction of viruses, worms, and some Trojan horse programs. These malicious programs can penetrate a computer network through the use of floppy disks, music CDs, infected web pages, file downloads over the Internet, and electronic mail. Unless your network has no internet connectivity, is on a closed network, does not use email, and has the floppy drives and CD-ROM drives disabled on all computers, you run the risk of infection unless you implement this software. It can be configured to automatically update itself over the Internet whenever new virus signature files are released. Virus signature files must be kept up to date with the latest versions in order for the software to provide good protection. These software packages can be purchased for each individual workstation, or in bulk license packs that may be cheaper for the organization. The computer hard drives should be scanned periodically, and all email and file downloads should also be scanned real-time. There are settings within the software to enable these functions. While there are numerous vendors of these products, some of the more popular ones are indicated in Table 2 on the next page along with the manufacturer's URL for further reference.

Table 2

McAfee VirusScan, NetShield, GroupShield, and WebShield	http://corporate.mcafee.com/content/suites/avd.asp
Norton AntiVirus™	http://enterprisesecurity.symantec.com/content/productlink.cfm#0
TrendMicro Officescan™	http://www.antivirus.com/products/osce/
Inoculan® for Microsoft Windows NT	http://ca.com/products/descriptions/inoculan_nt.pdf

One last problem that often occurs is the lack of protection for dial-up access. Vendors often install products that allow them to remotely access servers to perform maintenance or software upgrades. The problem is that unless properly managed, these connection points can circumvent any firewalls and leave a network very vulnerable to attack. An attacker will use a type of software called a wardialer to automatically look for phone numbers that are answered by modems. Once located, he can attempt to break into the computer that answers. Remote access software can make this very easy if password protection is not enabled along with other security features.

Dial-up software should be configured to require a user account for anyone dialing into the system. Passwords should be enabled on each account. The software should have similar account controls, as you would enforce in the Windows NT environment. Accounts should lock after a small number of failed login attempts. The connection should then terminate and not be allowed to resume with that account until the system administrator enables it. Account privileges should be limited to only those functions necessary for the vendor to perform. Automatic logging should be enabled on the software to record all activity for each session. The logs generated by the software should be reviewed. It is also a good idea to have someone monitor the software while the vendor or caller is on the system to make sure no unauthorized activity occurs. Remember that unless properly configured, people dialing in to a system with this software will have the same abilities as any user sitting at the computer, sometimes even more. A good measure to take with this type of configuration is to configure the phone line and modem for outgoing calls only and dial-back access and to disconnect the phone line from the computer modem when not in use.

Although this paper examines each area in general, it is provided as a beginning reference on what to do to start your agency down the path of system security. Enough resources are also referenced to assist the criminal justice agency in obtaining additional information to go beyond this level and take further steps to secure their systems. Remember that we are all responsible to secure the computer systems and networks that we use.

[1] National Cybercrime Training Partnership

[2] InfraGard

[3] Cullinane

[4]Smith

[5] Smith

[6] Smith

[7] Smith

[8] Smith

[9] Tarp

[10] Smith

[11] InfoSysSec Security Portal

[12] Fraser, Ed. 6

[13] Fraser, Ed. 10

[14]Fraser, Ed. 9

[15] International Information Security Foundation

[16]Carnegie Mellon University CERT/CC

References

Carnegie Mellon University CERT® Coordination Center. "Configure Firewall Logging and Alert Mechanisms." 01 May 2001. URL: http://www.cert.org/security-improvement/practices/p059.html (16 March 2002).

Cullinane, David. "ISSA – Information Systems Security Association." 6 March 2002. URL: http://www.issa.org (9 March 2002).

Fraser, B. Ed. "Site Security Handbook." September 1997. URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196 (16 March 2002).

InfoSysSec Security Portal. "Introduction to Physical Security." URL: http://www.infosyssec.org/infosyssec/physical_security.htm (10 March 2002).

InfraGard. "Welcome to InfraGard." 11 March 2002. URL: http://www.infragard.net (15 March 2002).

International Information Security Foundation. "Generally Accepted System Security Principles." June 1997. URL: http://web.mit.edu/security/www/GASSP/gassp021.html (16 March 2002).

National Cybercrime Training Partnership. "NCTP: Training." 5 March 2002. URL: http://www.nctp.org/training.html (9 March 2002).

Peltier, Thomas. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach Publications, 2002.

SANS Institute. "SANS Security Essentials." SANS Online Training. 2002. URL: http://www.sans.org/onlinetraining/track1.php (16 March 2002).

SANS Institute. "Track 9: SANS Information Security Officer." SANS2002 Annual Conference. 2001. URL: http://www.sans.org/SANS2002/track9.php (16 March 2002).

Smith, Danny. "Improving Computer Security through Network Design." 1997. URL: http://www.auscert.org.au/Information/Auscert_info/Papers/Security_Domains.html (11 March 2002).

Tarp, Keli. "Clues from Climatology: When and Where Do Tornadoes Occur?" 08 October 2001. URL: http://www.oar.noaa.gov/spotlite/archive/spot_climatology.html. 11 March 2002.