Global Information Assurance Certification Paper

Computer Security And The Law:
What You Can Do To Protect Yourself

By

Karen C. Poffenberger
Version 1.4b
GIAC Security Essentials Certification (GSEC)
Option 1
Date Submitted: 27 April 2004

Abstract

Working as a defense contractor, one knows the importance of security regulations and directives. However, do these regulations really protect our mission critical data? One would like to think so, but no – the answer is; it is really up to the security administrative team and the individual staff to ensure the security of systems. This paper will briefly discuss two important security regulations/laws important to the defense department; the impact of the regulations to security systems; and what an organization can do to protect mission critical data. These regulations:

- The Computer Fraud and Abuse Act of 1986 (Public Law 99-474)
- Computer Security Act of 1987 (Public Law 100-35)

indicate what is prohibited and in general what is required, but they do not detail what must be employed in your systems to ensure security of data. The security mechanisms described in this paper may not be all-inclusive or the only mechanisms available. This paper aims to describe basic mechanisms that can be employed by organizations to protect themselves from security events.

Introduction

All anyone has to do is visit any one of the leading computer security journals or the U.S. Computer Emergency Readiness Team's website (http://www.cert.org/) to realize the threat of cyber crime is very much alive. From the latest virus, worm, or email scandal to the full blown intrusion into a computer system, one can not help but conclude the threat is real. Although statistics prove the facts, one doesn't need them to know the threat exists. However, according to the Internet Fraud Complaint Center in 2003, "the center received over 120,000 online complaints through its website this year, an increase of 60% over 2002." [1]

If you haven't been the victim of a computer security event, count yourself lucky. The laws are supposed to be here to protect us, but what can we do to protect ourselves? This paper will hopefully present several basic security principles an organization can employ to offer protection against the various threats to critical data.

1.0 The Laws

As stated in the abstract, the laws to be discussed are:

- Public Law 99-474: The Computer Fraud and Abuse Act of 1986
- Public Law 100-235: The Computer Security Act of 1987

The Computer Fraud and Abuse Act of 1986

Public Law 99-474, US Code, Title 18, Section 30, is also known as the Computer Fraud and Abuse Act of 1986. The act was first passed in 1984, which has undergone several amendments. According to Burke, originally the act was aimed at protecting "classified information that was maintained on federal government computer, as well as

the protection of financial records and credit information on government and financial institution computers." [2]

In its present form, one can be fined or imprisoned for a wide variety of acts that compromise the security of public and private sector computers.

According to the Act, it makes it punishable by fine and/or imprisonment for anyone who:

1. Intentionally accesses a computer without authorization or exceeds authorized access and obtains financial information, United States department or agency information, or protected information from any protected computer involving interstate or foreign communication [3]
2. Intentionally accesses, without authorization a computer exclusively, or non-exclusively (if conduct affects use) used by the Government of the United States [4]
3. Knowingly with intent to defraud, accesses or exceeds authorized access a protected computer and steals anything of value, other than use of the computer itself and the value is not more than $5,000 in any 1-year period[5]
4. Knowingly, without authorization, transmits programs, information code, or commands which causes damage, causes physical injury, or threatens public health, national defense or national security [6]
5. Knowingly, without authorization, and with intent to defraud traffics in any passwords or similar information that involve interstate or foreign commerce or computers of the U.S. Government with attempts to extort money or items of value [7]

These crimes are punishable by fine, prison, or both. Depending on the exact crime, one can receive up to twenty years in prison.

The law defines a protected computer as "a computer exclusively used for a financial institution or U.S. Government, or conduct which affects the use of these computers."[8] In addition, the law defines exceeds authorized access as, "access to a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitles to obtain or alter." [9] Finally, it defines damage as "any impairment to the integrity or availability of data, a program, system or information." [10]

The Computer Security Act Of 1987

Public Law 100-235 is also known as the Computer Security Act of 1987. The purpose as described in the law is to "improve the security and privacy of sensitive information in Federal Computer Systems." [11]

This law basically requires every government computer system that contains sensitive information to establish a security plan and provide periodic mandatory training for all persons who manage, operate, or use these systems. This law also identifies NIST (originally the National Bureau of Standards) as the agency responsible for assessing

the vulnerability of Federal Computer systems, for develop standards, and providing technical assistance with NSA support.

The Law defines sensitive information as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or privacy of individuals." [12]

Impact of these laws

One of the laws described requires government agencies to create security plans and provide training; however, the law does not outline how an organization should complete these tasks. Neither law provides the necessary resources such as dollars, manpower, and time for organizations ensure they are compliant with the law. The Computer Fraud and Abuse Act is meant to outline punishable acts, but these seem to do little for the actual protection of our computer systems or deter hacking. This is evident in the ever growing number of viruses, worms, and intrusions.

2.0 What can an organization do to protect them selves

With these laws, one would think the Federal government knows exactly what to do to secure its networks and computer system. Well not exactly; according to the 2003 Federal Computer Security Report Card, "overall the Federal Government gets a grade of D," which is an improvement of 2002's grade of F." [13] It is not all bad though, the Nuclear Regulatory Commission and National Science Foundation received A's.

So what can an organization do exactly? The SANS (as outlined by Eric Cole in SANS Washington, Dec 8-13, 2003) promotes the concept that there are four core principles of Network Security, which in my opinion can be applied to any computer system. These four principles are as follows:

1 – Know Thy System
2 – Principle of Least Privilege
3 – Defense in Depth
4 – Prevention is ideal, but detection is a must.

Each principle will be discussed in detail, along with steps an organization can take to help protect the computer network and/or system.

3.0 Know Thy System

It is critical to know the details of the networks, printers, routers, hubs, and personal computer workstations that make up your computer configuration in your organization. If you don't know these aspects, how can you ensure it is protected? There are several keys to understanding and defining your system. They are as follows:

- Know entry points of access: where could someone potentially gain access
- Know what services are running: only employ those that are absolutely necessary and turn off all others

- Know what ports are open: absolutely shut down port 80 to incoming traffic if at all possible and any other port not necessary for completion of the organization's mission
- Possess a current and accurate network architecture diagram detailing all components of the systems including data flow across the network
- Know all hardware and software on all systems: Perform an inventory and periodically ensure it is accurate
- Perform a risk assessment to practice risk management

By documenting the entry points, an organization learns where the potential is for an intrusion. In addition, if these entry points can be protected by other means such as a firewall or intrusion detection system, then the organization is beginning the process of protecting its assets. The services that may be automatically turned on when an operating system is installed could spell security trouble. An installation straight out of the box, is not necessarily secure, that is why it is critical to examine all services that are running and shut those not necessary off.

Ports that are left open may allow an intruder to gain access. All ports both open and closed must be documented. It is also critical to ensure all ports get closed after any maintenance is performed; otherwise an unexpected intrusion could occur. In addition, close ports that are not necessary to complete the organization's mission so that administrators do not have to monitor and protect ports that are unnecessary.

A network architecture diagram will ensure that all components are detailed in a visual drawing. This diagram could become critical in a disaster recovery situation. This diagram will not only point out potential entry points, but also potential points of failure. By realizing the potential entry points and points of failure, an organization can place additional security measures at these locations. It will also detail all components in the network and how they interact with each other. In addition, it is helpful to document the data flow across the network so that you know what data you are trying to protect against information theft.

An inventory of all hardware and software will not only document an organization's assets, but also serve to document all systems and software that must be protected and maintained. This inventory will aid when performing upgrades, patches, and maintenance. An inventory will help ensure that all resources are upgraded, patched and maintained properly. Without an inventory, a critical asset could be missed during updates. Finally, an inventory will become invaluable should a disaster occur and it becomes necessary to rebuild the network structure, hardware, and software.

Finally, performing a risk assessment and performing risk management allows an organization to take the steps necessary to reduce risk to an acceptable level. In their book, SANS Security Essentials with CISSP CBK, Volume 1, Cole, Fossen, Northcutt, and Pomeranz define risk as follows:

"RISK = THREAT x VULNERABILITY

where vulnerability is defined as a weakness in a system that could be exploited; while a threat is any event that can cause an undesirable outcome." [14, p.832]
An administrator's job is to assess the risk for each asset that you identify needs protecting. Once you identify and assess risks, you can determine an accept level of risk to manage them.

Threats show you what vulnerabilities to key in on. Threats can be natural, human, or environmental. In addition, they can come from outside or inside your organization, with the inside threat potentially causing the most severe damage to the system. Malicious code, hackers, worms, viruses, and emails with suspicious attachments are potential threats. Other threats include such events as fire, flood, earthquakes, or any other natural disaster. Finally, user error could also be considered a threat because it has the potential to cause damage to your mission critical data. It is critical to stay familiar with threats and vulnerabilities so that an organization knows what they must protect against.

A risk assessment will help identify both the threats and vulnerabilities. During a risk assessment, the key areas to consider are: [15][16]

- Identifying applications critical to business
- Who can use them
- Where users will access them from
- Devices used to access these applications
- How application security fits into corporate business continuity plan
- Hardware and software
- System interfaces
- Data and information
- People who support the system
- System mission
- System and data criticality
- System and data sensitivity

According to NIST, "risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level."[17] It is important that organizations determine what is acceptable and begin the process of managing risks to the accepted level so as to minimize loss or damage.

4.0 Principle of Least Privilege

Cole, Fossen, Northcutt, and Pomeranz define least privilege as "the smallest amount of privilege necessary for performing a particular job." [18, p.388]

Along with least privilege is the need to know. This is especially critical in a government setting. Although one may possess a top secret clearance, he/she should not be given access to all secret documents, but only those relevant to the job duties. This is due to the fact that although they may possess the proper clearance, they may not have the need to know or see all the information stored on the system.

The need to know concept "ensures that only people that have a need to access certain information or resources will be authorized to do so. In addition, least privilege is similar in that it "ensures that only the minimum required access is given at any one time." [19, p.1105]

This least privilege should be employed on all systems: read, write and execute. In addition, when a user no longer needs privileges, they should be relinquished immediately. This ensures that a user can not accidentally access a document they should not see.

To employ this concept in an organization, the administrators should review the needs of all users to ensure they have the ability to access those documents they need to perform their job function, but not access those that are unnecessary to performing their duties. These privileges can be documented in an access table indicating which privileges are provided to each user, such as read, write, execute or delete. These privileges can be employed to the individual document level if necessary. Caution should be exercised so that when privileges are no longer needed, they are relinquished. In addition, if a user leaves an organization, his/her privileges should be removed immediately. Finally, it is best to document procedures for adding, modifying, or removing users to the system and granting, modifying, and removing privileges of users.

5.0 Defense in Depth

In practicing defense in depth, an organization employs multiple layers of security protection so that if one component fails, there are other measures to continue protecting the systems.

An organization should find an acceptable balance between the protection capabilities and cost and operational considerations for employing these capabilities. According to NSA, "an important in depth strategy is that achieving Information Assurance requires a balanced focus on three primary elements: people, technology, and operations." [20]

According to Netscreen Technologies, there are several benefits in practicing defense in depth which include: harder for intruders to penetrate all defenses, reducing the likelihood of a complete security breach, minimizing time required to detect and react to intrusions and attacks, accelerating the deployment of modular security architectures, and lowering expenditures by using commercial off-the-shelf (COTS) products. [21]

Organizations need to be prepared in the event of an attack. They need to employ multiple layers of security measures. In addition, detection mechanisms should be put in place along with written procedures to react to and recover from an attack. By having multiple layers of security measures in place, in the event of an attack, these layers could potentially buy time to respond to an attack and hopefully minimize the damage sustained. These multiple layers would give an administrator time to react and

prevent further damage. To have controls, but not monitor them would be useless. It is critical that these controls are properly installed and configures as well as administrators properly trained in the use, monitoring, and identification and reaction to potential intrusion on these layers of protection. In my opinion, an organization can never have too many layers of security or too much training.

Although some of the mechanisms can also be considered prevention, there are several security mechanisms that can be implemented to accomplish defense in depth which will be discussed below:

- Firewalls
- Identification, Authentication, and Authorization
- Encryption
- Separation of Servers and Duties
- Routers and Switches
- Physical Security measures
- Training
- System Monitoring and Auditing
- Installation, maintenance, patch and upgrade procedures
- Hardening the Operating system
- Content filtering

Firewalls

Firewalls are typically the first layer of security by controlling who and what has access to the network. According to Cole, Fossen, Northcutt, and Pomeranz, firewalls should be located at intersections of traffic for: [22, p.42]

- private systems to the internet
- private to semi public servers
- semi public to internet
- internet to semi public servers

In addition, nested firewalls at inner and outer network boundaries can provide double protection. Perhaps a bit overkill, but personal firewalls can be placed on each personal computer. However, this could become an administrative nightmare unless you have a mechanism in place (such as SMS) to push out technology updates and patches to each computer on the network. Finally, an organization may want to use different types of firewalls at the various layers. For example, an organization may use a packet filtering firewall at the outer most layer of the system and an application level gateway, or stateful inspection on another layer. These in combination may offer a greater defense to the network. A packet filtering firewall can be placed at the gateway or outer perimeter. This allows for maximum throughput, because only up to layer three (3) of the OSI model is checked. This type of firewall operates only on the IP header of a packet to determine where it came from, where it is going, and what kind of connection it wants to make. The drawback of this type of firewall is the fact that it does not know the difference between real and forged addresses. An application level gateway verifies contents of the packet all the way through the application layer, layer seven (7), of the OSI model, not just the IP header. It intercepts both incoming and outgoing packets.

Stateful inspection firewalls store information in memory about the state of current sessions and checks its tables when packets are received in response to a request sent out to ensure that the packet is indeed a response to the request. [23, p.95] However a firewall alone can not defend against all attacks. This is only one type of defense that can be put in place.

Identity, Authentication, and Authorization

It is critical that the identity of each user, program, computer, or data is established, so that actions can be tracked by each. Each user must also have an authentication mechanism. The most widely used is the password. Organizations should stress the importance of strong passwords. The latest Army standard calls for a password length of at least 10 characters containing a mix of uppercase and lower case letters, numbers, special characters. These passwords must contain at least two of each of the four types of required characters and should not be associated with the individual in any way. In addition, they recommend password be changed at least every 90 days. [24] By entering the identity and authentication, the system can verify they are valid and be able to determine what they are authorized to perform.

Encryption

To help provide confidentiality and integrity of data, encryption should be used. Not only should passwords be encrypted when passing them across the network, the database that houses them should also be encrypted. This would make it more difficult for the hacker to gain access into the database that houses user passwords. In addition, an organization may want to consider encrypting critical email messages in an effort to stop a potential hacker from reading the message. Finally, an organization may choose to encrypt critical files when storing or transferring them across the network.

Separation of Servers and Duties

It is critical that servers that serve different purposes are separated. The email server should be separate from the web server as well as the Domain Name System server. This separation makes it difficult for an intruder to access all servers in one hit. In addition, administrative duties should be separated among multiple staff members so that one person does not have total control over the network resources.

Routers and Switches

Like a firewall, a router can filter out unwanted traffic. An organization can develop an access control list (ACL) for the router so that unwanted traffic can be denied at the perimeter. This ACL can include known addresses for hacking activities. If possible, use switches instead of hubs because they are hard to sniff effectively. Switches combine hub and bridge functionality.

Physical Security measures

Physical security is often an after thought or completely overlooked. This concept will be discussed in depth in Section 6.0, Prevention is ideal, but detection is a must. Simple mechanisms such as locks, badges, motion sensors, and fences can all be employed to deter unauthorized access.

Training
People are critical to your security; they can make or break it. Proper training and awareness is a must. They must understand your security policy; not just read it and toss aside. Establish policies and procedures and ensure all employees are fully trained on not only the policy, but any consequence for unacceptable actions. Training will be further discussed in the next section, Prevention is Ideal, But Detection is a Must.

System Monitoring and Auditing
Auditing itself can not prevent security violations, but it can be useful in establishing and documenting the source of the violation and assessing the extent and nature of the damages sustained. This concept will be further described in the next section.

Installation, maintenance, patch and upgrade procedures
Procedures should be documented for testing and installing patches and upgrades. Included in patches and upgrades are virus signature definitions which should be kept up to date. Although we can get busy with every day tasks, it is critical not to ignore warnings from the CERT advisory. These are often critical to the success of the security of your data. All patches, fixes, and upgrades should be first completed on a "test" server so that any impacts can be identified to ensure that a new patch, fix, or upgrade does not open your organization up to any new security vulnerabilities.

Hardening the Operating System
Most operating systems contain security flaws. In addition, if you install the operating system with the defaults that ship with the original software, you could open your organization up to potential security concerns. Hardening an operating system helps to remove potential vulnerabilities. During the hardening process, it is important to turn off all unnecessary services. In addition, it is critical to secure access controls using the principle of least privilege concept. All administrator, guest, and unnecessary accounts should be removed so that potential intruders can not search for the specific account called "administrator."

Content filtering
To help ensure unwanted emails and attachments do not make it through your system, an organization should monitor their email attachments and block any email that poses a threat to the organization. For example, an organization should consider blocking emails whose attachments are of the following types: executable files (.exe or .com), batch files (.bat or .cmd), scripts which can take several forms (.vbs, .vs, .vb, etc), or screensavers (.scr). At a minimum, organizations should filter for spam type emails or known adult content mails. If an organization does not automatically perform this, it is recommended that users enable email rules if their email application allows filtering out their own spam, adult content and inappropriate email content. In addition, an organization should block users from visiting inappropriate web sites. However, the only way to stop the spread of email viruses and inappropriate sites is to restrain from opening suspicious emails and block inappropriate websites.

In summary, there is no one magical solution that will guarantee that your critical assets will be protected, that is why it is important to employ the concept of defense in depth. By employing multiple mechanisms, an organization can hopefully minimize damage from an attack, and gain valuable time to protect their data should an attack against one mechanism occur.

6.0 Prevention Is Ideal, But Detection Is A Must.

The key to security is to try and prevent security events. However, not only should prevention be instilled, but detection as well. In order to respond to incidents, you must be able to detect them. Finally, once you detect an incident, you must be prepared to respond. The techniques discussed in the previous section can all be considered prevention mechanisms. Additional information about these mechanisms will be provided in this section. Other prevention techniques will also be discussed. In order to respond to a security event, an organization must have detection mechanisms in place as well as recovery plans.

Prevention

It would be ideal if we could prevent all security events; however, we all know that is impossible. Organizations can introduce several mechanisms that are preventative in nature. These mechanisms will be discussed below and include:

- Training
- Preventing Attacks from Within
- Antivirus Protection
- Passwords
- Physical Security
- Content Filtering and Website Blocking
- Firewalls
- Intrusion Detection Systems
- Configuration and Change Control
- Plans, Policies, and Procedures
- Penetration and Vulnerability Testing

Training

In my opinion, training is a must. All staff in the organization must be trained. Employees should learn why security is important and their role in helping prevent security events. In addition, all employees should be trained in the security policy. If you make employees feel as though they have a part in protecting the critical data, they will be more willing to provide information should an event occur. Topics such as: threats not only of hacker, but email viruses, as well as intruders into the building (physical security), fire, flood, etc. should be included. Teach employees not to open suspicious emails with attachments. Don't forget about physical security. Employees should know what to do if any are breached. Let them know what is appropriate and inappropriate behavior on the internet. They should know that all traffic is logged and monitored. Employees should be taught to never share passwords with anyone, especially someone on the telephone. This is a type of social engineering that a

potential hacker could use to gain access into a system. Training should also include periodic refresher training. National Institute for Standards and Technology developed a special publication (SP-800-50) that outlines what an organization should do to design, develop, implement, and maintain an Information Technology (IT) awareness and training program. This publication outlines awareness topics which include the following: (not all inclusive) [25]

- Password usage
- Protection from Viruses
- Policies
- Web usage
- Incident response
- Personal Digital Assistant (PDA) security issues
- Laptop security while on travel

In addition, it details techniques for delivery and training including: [26]

- Posters
- Warning banners
- Newsletters
- Instructor led classes, computer based training, videotapes, or seminars
- E-mail messages

Finally, the Appendices in Special Publication 800-50 offer Sample Awareness Training Plan Templates (Appendix B) as well as Sample Posters (Appendix C).

Attacks from Within

Attacks from within are costly and could potentially cause severe damage. Steps must be taken to prevent these attacks. To minimize attacks from within, an organization can employ the principle of least privilege. This will provide users with only the resources necessary to perform their job functions.

Antivirus Protection

A key measure in protecting security events on computers is to install antivirus software on all machines. However, it should not stop simply with the installation. It is critical that the virus signatures are kept up to date. If they become out of date, a virus could be spread throughout an organization.

Passwords

As detailed in the previous section, it is important for organizations to require strong passwords. A best practice security measure is to lock users out of the system after three invalid attempts. Employees should only be allowed back in after it is determined the reason for the failure. As previously discussed, users should be required to select passwords at least 10 characters in length mixing a combination of upper and lower characters, numbers, and special characters.

Physical Security

Physical security is often overlooked in an organization. Several physical security measures that are important will be mentioned. It is critical to control access to the room that houses the organization servers. The server room should be designed with backup generators, air conditioning, and humidity control systems. In addition, users should protect laptops from theft at all times. A cheap method to identify employees is to use a badging system. A little more advanced, but will go along way to provide security is to have a badging system that users would swipe their badge to enter the building and floors/rooms in the building. To prevent unauthorized access while away from your computer, users should be required to use password enabled screen savers that should activate after 30 minutes of inactivity.

Content Filtering and Website Blocking

As previously discussed, emails attachments should be scanned and blocked accordingly to prevent the spread of viruses, malicious code, and spam. Inappropriate websites should be blocked to avoid employees from potentially visiting sites that may have potential for causing harm.

Firewalls

Firewalls, as previously discussed act as a perimeter guard by determining what traffic to let in or deny in and out of the network.

Intrusion Detection Systems (IDS)

Intrusion detection systems monitor network traffic, looking for patterns indicative of an attack on a computer. IDS systems can detect activities such as port scan or denial of service (DOS) attacks. Intrusion Detection Systems can be either network or host based. Although, perhaps more effort than a network based IDS, due to the fact that software must be installed on every host, the advantage of a host based IDS is that it can detect backdoors into a network. It can also detect intrusions that Network Based IDS's often miss. Network based IDS's typically watch traffic that crosses the borders of the network giving you the ability to see network traffic across the entire network and can spot anomalies which could indicate a potential attack. [27, p.754] If possible, a combination of both host based and network based intrusion detection systems, would provide an organization with optimal intrusion prevention.

Configuration and Change Control

All organizations should have a configuration management and/or change control policy to ensure that network changes, additions, etc. are performed in a consistent and controlled manner and are thoroughly documented. Changes to the system and patches/fixes must be tested to ensure they do not cause negative impact to the security of the system. In addition, these changes should be documented and approved before they are completed. Any new change or "fix" should be first loaded on a test server before being completed in the production environment so that you can make sure that you do not open up any new vulnerabilities with the change.

Plans, Policies and Procedures

To ensure success, organizations should develop policies and procedures for security. At a minimum, organizations should develop the following policies and/or procedures:

- Security Policy
- Password Policy
- Incident Response Plan
- Disaster Recovery Plan
- Configuration and Change Control Policy
- Auditing Procedure
- Document who has access to what resources on the network
- Monitoring procedures
- Audit checklists

These policies are very important to the overall security of an organization. These policies should be reviewed periodically to ensure they are up-to-date and continue to be accurate. At a minimum, employees should be trained on the security and password policies. When developing these policies and procedures an organization should make sure they are in compliance with all applicable laws and regulations to which they must adhere. These policies should be clearly written and detail the consequences of non-compliance. It is critical that justification is provided in each policy. Documented procedures will ensure that the staff performing the duties will follow the same methods every time they perform the procedure. In addition, these documented procedures will help eliminate potential errors.

Penetration/Vulnerability Testing

By performing penetration testing on the network, the administration team will be able to point out and report all vulnerabilities on the system. This will allow the organization to recognize vulnerabilities and employ additional security measures against them. This vulnerability scanning will provide an organization with a hacker's eye view of the network perimeter and point out weaknesses so that administrators can weigh the risks and eliminate potential opportunities for hackers to gain access into the network resources.

Detection and Recovery

Since we know it is impossible to prevent all security incidents, then an organization must be prepared to detect and respond to a security incident. Organizations can incorporate detection and recovery mechanisms into their overall security strategy which include:

- Auditing and Monitoring
- Intrusion Detection Systems (IDS)
- Backups
- Recovery and Response Plans

Auditing and Monitoring

Auditing and monitoring of all system resources is a must. Auditing can trace a user's actions, assists in determining unauthorized access in addition providing real-time monitoring of systems. In addition, it helps support after-the-fact investigations. Audit trails are critical for detection and investigation of security incidents. Audit trails can provide information such as: what occurred, when it occurred, who caused it, how the event was detected, and when the event was detected.

Audit trails can contain both successful events and failure events. Audit event records contain information such as the user id, date and time of log on and off, identity such as terminal, IP address or location, record of transaction, type of violations and consequences, and time of occurrence. There are various tools available that can aid in the audit process and detect deviations. To ensure all staff performs auditing consistently, procedures need to be established for the type and frequency of audits as well as procedures for auditing and reporting potential incidents. These audit trails should be reviewed regularly. In addition, they should be backed up. Finally, you should ensure that they have not been modified, deleted, or altered so that should an event occur, you have accurate data to serve as evidence as an attack.

It is important to both audit and monitor. Monitoring is performed to identify unauthorized access attempts, whereas auditing "verifies the security and resources and also whether or not a system has been compromised or misused" [28, p.1110]

IDS

As previously stated, an Intrusion Detection System monitors network traffic, looking for patterns indicative of an attack on a computer. An IDS alerts you when a potential attack is in progress by indicating what is under attack, how the attack is occurring, source of the attack, and signature of attack. Once a potential attack is detected, it can perform the following to alert administrators: email notification, send a page to a pager, block or kill a TCP connection, send an SNMP trap to a network management system, or run a user defined script.

Backups

Although a prevention mechanism, backups are also critical in the recovery from an incident. Backups should be performed daily. The data should be stored offsite so that if a disaster were to occur in the primary building, data stored offsite could be used to bring systems back online after a disaster. Data restore should be performed to ensure that in the event of a disaster, data can be restored successfully. Restoring should be performed on a regular basis to ensure success when needed.

Recovery and Response Plans

All organizations should have in place a system for reporting problems and recovering from an incident. In planning and recovering from an incident and organization should perform the following: [29]

- Have a plan and even perhaps rehearse it
- Identify the affected computers
- Contain the problem to prevent further problems
- Eradicate and fix the problem
- Recover from the attack/infection
- Learn from mistakes and prepare a lessons learned to share experiences with others

The recovery plan must include easy to follow details to help alleviate stress and prevent mistakes from occurring. It is also helpful to have a disaster recovery tool bag that contains such items as: cables, hubs, wire cutters, and software to name a few. It is critical to use these materials for recovery and replenish this bag after an incident.

7.0 Summary and Conclusion

I hope by reading this paper you have gained a basic understanding of two key security regulations/laws, but more importantly some of the basic mechanisms an organization can employ to better protect themselves from a computer event. As technology continues to advance, so does the need to protect our most valuable assets: our mission critical data.

APPENDIX A – SUMMARY LIST OF SECURITY MEASURES

This appendix provides a summary list of the security measures mentioned in this paper. Using this list, an organization can begin to take the proper steps necessary to protect themselves from security incidents.

1. Know the entry points of access
2. Determine services that are running and disable all unnecessary services
3. Know which ports are open and block all unnecessary ports
4. Possess a current network architecture diagram
5. Inventory all hardware and software on the system
6. Perform a risk assessment and practice risk management
7. Practice the Principle of Least Privilege
8. Employ Firewalls at multiple levels and entry points
9. Encrypt passwords, critical emails and files
10. Separate Servers that perform different functions as well as administrative duties among staff members
11. Use routers and switches wisely
12. Don't forget about Physical Security Measures
13. Training, Training, and More Training
14. Monitor and Audit systems
15. Installation, Maintenance, patch and upgrade procedures
16. Harden the Operating System
17. Filter email attachments and block inappropriate websites
18. Prevent Attacks From within by employing least privilege
19. Employ Intrusion Detection Systems
20. Install Antivirus software on every computer and keep the signatures up-to-date
21. Encourage strong passwords and change them at least every 90 days
22. Practice Configuration and change control
23. Develop Plans, Policies, and Procedures
24. Perform Penetration and Vulnerability testing
25. Backup data regularly and make sure it can be restored effectively
26. Recovery and Response Planning

References

1. Poulsen, Kevin. “Online Crime up in 2003.” 24 December 2003.
   URL: http://www.securityfocus.com/news/7714

2. Burke, Edmund B. (Peter). “The Expanding Importance of the Computer Fraud and Abuse Act.” January 2001
   URL: http://www.gigalaw.com/articles/2001-all/burke-2001-01-all.html

3. “Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 – Fraud and False Statements, 1030. Fraud and Related Activity in Connection with Computers.” Title 18, United States Code Annotated, Title 18. Sec 1030. [2 a-c]
   URL: http://uscode.house.gov/DOWNLOAD/18C47.DOC

4. “Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 – Fraud and False Statements, 1030. Fraud and Related Activity in Connection with Computers.” Title 18, United States Code Annotated, Title 18. Sec 1030. [3]
   URL: http://uscode.house.gov/DOWNLOAD/18C47.DOC

5. “Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 – Fraud and False Statements, 1030. Fraud and Related Activity in Connection with Computers.” Title 18, United States Code Annotated, Title 18. Sec 1030. [4]
   URL: http://uscode.house.gov/DOWNLOAD/18C47.DOC

6. “Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 – Fraud and False Statements, 1030. Fraud and Related Activity in Connection with Computers.” Title 18, United States Code Annotated, Title 18. Sec 1030. [5]
   URL: http://uscode.house.gov/DOWNLOAD/18C47.DOC

7. “Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 – Fraud and False Statements, 1030. Fraud and Related Activity in Connection with Computers.” Title 18, United States Code Annotated, Title 18. Sec 1030. [6-7]
   URL: http://uscode.house.gov/DOWNLOAD/18C47.DOC

8. “Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 – Fraud and False Statements, 1030. Fraud and Related Activity in Connection with Computers.” Title 18, United States Code Annotated, Title 18. Sec 1030. [Definitions e2]
   URL: http://uscode.house.gov/DOWNLOAD/18C47.DOC

9. “Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 – Fraud and False Statements, 1030. Fraud and Related Activity in Connection with Computers.” Title 18, United States Code Annotated, Title 18. Sec 1030. [Definitions 6]
   URL: http://uscode.house.gov/DOWNLOAD/18C47.DOC

10. "Crimes and Criminal Procedure, Part I – Crimes, Chapter 47 – Fraud and False Statements, 1030. Fraud and Related Activity in Connection with Computers." Title 18, United States Code Annotated, Title 18. Sec 1030. [Definitions 8]
URL: http://uscode.house.gov/DOWNLOAD/18C47.DOC

11. "The Computer Security Act of 1987." Public Law 100-235, H.R. 145 Section IV. Explanation of the Bill, Purpose, 8 January 1988.

12. "The Computer Security Act of 1987." Public Law 100-235, H.R. 145, Section IV. Explanation of the Bill, 8 January 1988.

13. United States Congressional House. Committee on Government Reform. 2003 Federal Computer Security Report Card. Hearing, 9 December 2003. 107th Congress.
URL: http://reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=652

14. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Volume 1 version 2.1. SANS Press. April 2003. 832.

15. Lee, Mike. "Protecting Yoyr Business in the Right Places – Security Applications." October 10, 2003.
URL: http://www.itsecurity.com/papers/bt2.htm

16. Stoneburner, Gary. Goguen, Alice. Feringa, Alexis. National Institute of Standards and Technoogy (NIST) Special Publication 800-30. "Risk Management Guide for Information Technology Systems." October 2001
URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

17. Stoneburner, Gary. Goguen, Alice. Feringa, Alexis. National Institute of Standards and Technoogy (NIST) Special Publication 800-30. "Risk Management Guide for Information Technology Systems." October 2001
URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

18. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Volume 1 version 2.1. SANS Press. April 2003. 388.

19. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Volume 2 version 2.1. SANS Press. April 2003. 1105.

20. Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments.
URL: www.nsa.gov/snac/support/defenseindepth.pdf

21. Defense in Depth: A Strategy to Secure Federal Networks. Netscreen Technologies, Inc. March 2003

URL: www.netscreen.com/dm/techpubs/downloads/wp_def_in_depth.pdf

22. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Volume 1 version 2.1. SANS Press. April 2003. 42.

23. Ogletree, Terry William. Practical Firewalls. QUE Corporation. 2000. 95.

24. Army Regulation AR 25-2. "Information Management: Management of Subdisciplines – Information Assurance." Headquarters – Department of the Army, Washington, DC. 14 November 2003

25. Wilson, Mark. Hash, Joan. National Institute of Standards and Technology (NIST). Special Publication 800-50. "Building an Information Technology Security Awareness and Training Program." October 2003.

26. Wilson, Mark. Hash, Joan. National Institute of Standards and Technology (NIST). Special Publication 800-50. "Building an Information Technology Security Awareness and Training Program." October 2003.

27. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Volume 1 version 2.1. SANS Press. April 2003. 754.

28. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Volume 2 version 2.1. SANS Press. April 2003. 1110

29. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK Volume 2 version 2.1. SANS Press. April 2003. 1086