

Developing a Computer Security Incident Response

- Define your organization's overall incident response structure.
- Develop and implement alert mechanisms that permit quick action.
- Establish a centralized reporting structure.
- Appoint and train incident response personnel.

Recognizing Signs of an Intrusion

- Observe your systems for unexpected behavior or anything suspicious.
- Investigate anything you consider to be unusual.
- If your investigation finds something that isn't explained by authorized activity, immediately initiate your intrusion response procedures

Monitoring Systems for Intrusion in a Windows Environment

- Look for unusual or unauthorized user accounts or groups.
- Using the computer management tool, check all groups for invalid user membership
- Check log files for connections from unusual locations or for any unusual activity.
- Search for invalid user rights.
- Check to see if unauthorized applications are running.
- Examine the Windows Registry.
- Look for invalid services.
- Monitor system startup folders.

NIPC Recommendations for Incident Victims

- Respond quickly. Contact law enforcement officials.
- If unsure of what actions to take, *do not* stop systems processes or tamper with files. This may destroy traces of an intrusion.
- Follow organizational policies/procedures. (Your organization should have a computer incident response capability/plan.)
- Use the telephone to communicate. Attacker(s) may be capable of monitoring e-mail traffic.
- Contact the incident response team for your organization. Quick technical expertise is crucial in preventing further damage and protecting potential evidence.
- Consider activating Caller Identification on incoming lines. This information may help in leading to the identification of the source/route of intrusion.
- Establish points of contact with general counsel, emergency response staff, and law enforcement officials. Pre-established contacts will help in a quick response effort.
- Make copies of files an intruder may have altered or left behind. If you have the technical expertise to copy files, this action will assist investigators in determining when and how the intrusion may have occurred.
- Identify a primary point of contact to handle potential evidence.
- Establish a chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. Potential hardware/software evidence that is not properly controlled may lose its value.
- Do not* contact the suspected perpetrator.

Incident Reporting Assessment

Low-level incidents are the least severe and should be resolved within one working day after the event occurs. These include

- Loss of passwords
- Suspected unauthorized sharing of accounts
- Misuse of computer hardware
- Unintentional computer actions
- Unsuccessful scans or probes

Mid-level incidents are more serious and should be handled the same day the event occurs (normally within two to four hours of the event). These include

- Property destruction related to a computer incident
- Illegal download of copyrighted music/unauthorized software
- Violation of special access
- Unauthorized use of a system for processing or storing personal data
- An act resulting from unfriendly employee termination
- Illegal building access
- Personal theft (moderate in value) related to a computer incident

High-level incidents are the most serious. Because of the gravity of these situations and the likelihood of damage resulting to the organization's bottom line, these types of incidents should be handled immediately. They include

- Property destruction related to a computer incident
- Child pornography
- Pornography
- Personal theft (higher in value than a mid-level incident) related to a computer incident
- Suspected computer break-in
- Denial of Service (DoS) attacks
- Illegal software download
- Malicious code (for example, viruses, worms, Trojan horses, and malicious scripts)
- Unauthorized use of a system for processing or storing of prohibited data
- Changes to system hardware, firmware (for example, BIOS), or software without the system owner's authorization
- Any violation of the law

Preparing Systems for Data Collection

- Enable logging and auditing on all workstations and servers.
- Make all workstations and servers time-synchronized with a reliable and accurate Internet timeserver, such as www.time.nist.gov.
- Use time-stamping and ensure that the verification of time stamps within your system cannot be modified or distorted.
- Identify network devices by creating a network map to serve as a baseline and graphical representation of the devices on your network for future reference.

IT Contingency-Planning Process

- Develop the contingency-planning policy statement.
- Conduct the business impact analysis (BIA).
- Identify preventive controls.
- Develop recovery strategies.
- Develop an IT contingency plan.
- Plan testing, training, and exercises.
- Plan maintenance.

NIST Forensic Tool Requirements

- The tool shall not alter the original disk.
- The tool shall be able to access both IDE and SCSI disks.
- The tool shall be able to verify the integrity of a disk image file.
- If there are no errors accessing the source media, then the tool shall create a bit-stream duplicate of the original disk or a disk partition on fixed or removable media.
- If there are I/O errors accessing the source media, then the tool shall create a qualified bit-stream duplicate. (A *qualified bit-stream duplicate* is defined to be a duplicate except in identified areas of the bit-stream.) The identified areas are replaced by values specified by the tool's documentation.
- The tool shall log input/output (I/O) errors, including the type of error and location of the error.
- The tool shall be able to access disk drives through one or more of the following interfaces: direct access to the disk controller, Interrupt 13 BIOS interface, Interrupt 13 BIOS extended interface, ASPI SCSI interface, or Linux interface.
- Documentation shall be correct insofar as the mandatory and any implemented optional requirements are concerned. For example, if a user following the tool's documented procedures produces the expected result, then the documentation is deemed correct.
- The tool shall copy a source to a destination that is larger than or equal to the size of the source, and shall document the contents of the areas on the destination that are not part of the copy.
- The tool shall notify the user if the source is larger than the destination

Dealing with Digital Evidence Obtained from a Memory Dump

- All of the standard forensic and procedural principles must be applied.
- Upon seizing memory-related evidence, actions taken should not change that evidence.
- People who access original digital evidence should be trained for that purpose.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- Individuals are responsible for all actions taken with respect to digital evidence while such evidence is in their possession.
- Any individual or group that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for complying with these principles.
- No potential evidence is damaged, destroyed, or compromised in any way by the procedures used to investigate the computer.
- Extracted and possibly relevant evidence is properly handled and protected from later physical or magnetic damage.
- A continuing chain-of-custody is established and maintained.
- Business operations are affected for a limited amount of time, if at all.
- Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

Detecting Malicious Code and Intruders

- Analyze any abnormal system processes using the Windows Task Manager or third-party tools like Process Explorer.
- Detect unusual or hidden files by modifying Windows to display certain hidden file types.
- Locate rootkits and backdoors in Unix and Linux by using third-party programs like Intact by Pedestal Software or via manual inspection.
- Scan for backdoors and network sniffers using the `netstat -n` and `ifconfig -a` commands.

Collecting Log File Data

- The process names and startup times
- The status of the process
- Which user executed the process
- The amount of system resources used by specific processes over time
- System and user processes and services executing at any given time
- The method by which each process is normally started and what authorization and privileges have been assigned to those processes
- Hardware devices used by specific processes
- Files currently opened by specific processes

Reviewing Operating System and Network Logs

Look for the following:

- Processes consuming excessive resources
- Processes starting or running at unexpected times
- Unusual processes not the result of normal authorized activities
- Processes that prematurely terminate
- Previously inactive user accounts that suddenly begin to spawn processes and consume computer or network resources
- Unexpected or previously disabled processes, which may indicate that a hacker or intruder has installed his own version of a process or service
- A workstation or terminal that starts exhibiting abnormal input/output behavior
- Multiple processes with similar names
- An unusually large number of running processes

Retrieving and Analyzing Clues

- Perform keyword searches using third-party tools like Disk Investigator or BinTex.
- Locate and examine the Windows swap file for evidence. Under Windows 95/98/ME, the swap file is called `win386.swp`, and in Windows NT/2000/XP, it is called `pagefile.sys`.
- Locate and retrieve e-mail evidence. E-mail messages can be found in a number of different places, such as the sender's e-mail inbox/outbox, a network server's mailbox, or backup media.
- Recover evidence from Web browser cache and history. Web caches reveal a lot about which Web sites a user has visited. Most contemporary Web browsers (for example, Internet Explorer and Netscape Navigator) perform Web caching and maintain browsing history.
- Gather evidence from the Windows print spooler (EMF) files. Even if a user never saved a word-processing document, temporary versions of word-processing documents sometimes remain on the hard drive.
- Locate data in hidden or masked file extensions. Be sure to scan for evidence hidden in steganographic images and password-protected compressed files.

Basic Procedures for Collecting and Preserving Evidence

- Understand volatility of evidence. Some evidence, such as data in the computer's RAM, only exists while the computer is powered on.
- Create a real-mode boot disk, because the simple act of turning on the computer can destroy potential evidence. By using a special real-mode boot disk, a forensic investigation can be conducted without booting the computer via the hard drive.
- Use packet sniffers to gather evidence. Computer investigations sometimes warrant the capture of "live" data as it travels in real time across an organization's computer network.
- Build a forensic toolkit. Essential to any computer investigation, toolkits come in two types; those you assemble yourself and pre-fabricated ones that you download or purchase as a suite from any one of many forensic software vendors.
- Follow a chain-of-custody. The chain-of-custody is a record of evidence handling from the time of seizure to the time evidence is presented in a court of law.
- Ensure the admissibility of evidence collected via authentication. Before a computer record can be used as evidence, it must first be proven to be authentic.

Computer Evidence Guidelines

- Admissible. The evidence must conform to certain legal rules before it can be put before a court.
- Authentic. It must be possible to positively tie the evidentiary material to the incident by showing that the evidence relates to the incident in a relevant way.
- Complete. It must tell the whole story and not just one particular perspective. Not only should you collect evidence that can prove the attacker's actions, but also evidence that could prove his or her innocence.
- Reliable. There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.
- Believable and understandable. The evidence must be readily believable and understandable by a court of law.

The Order of Evidence Collection

- Find the evidence. Figure out where the evidence you are seeking is being stored on the system.
- Determine data relevance. Decide what parts of the data you collect are relevant to the case at hand.
- Rank volatility. Items that are most likely to degrade or become unusable should be collected first.
- Eliminate outside interference. As only unaltered data may be entered as evidence, utmost care must be taken to thwart any possible outside contamination.
- Collect the evidence. As you gather evidence, continue to examine the items you've already collected, as new pieces you collect may influence what you consider worthy information.
- Document everything. Your method of collecting the evidence you present may be called into question later, so be sure to maintain a record of everything that you've done in the collection process.

Collecting Volatile Evidence

- Do not power down the system until you have completed all the evidence collection procedures for volatile evidence.
- Don't trust the programs on the system. Intruders have been known to replace system commands.
- Don't run programs that modify the access time of all files on the system.
- When removing outside interference, keep in mind that simply disconnecting from the network may trigger a dead-man switch that can detect when the computer is disconnected from the network and quickly delete evidence.

Building an Incident Response/Forensic Toolkit

A properly outfitted toolkit enables its owner to efficiently collect evidence for later analysis and should contain the following elements:

- A tool to capture network traffic for analysis (for example, a network sniffer)
- A utility to create disk images or clones at the bit level
- A tool to crack passwords
- A tool that reports open TCP/IP ports and then maps them back to their owning process
- A tool to recover deleted (erased) data
- A data collection tool to capture file slack and unallocated (erased file) data
- A tool to discover hidden files, such as NTFS Alternate Data Streams
- A monitoring tool that displays all Registry activity in real time
- A utility to back up and edit the Windows Registry
- A tool that displays open files, object processes, Registry keys, DLLs, and owners of object processes
- A utility to display all file system activity in real time
- A tool to analyze file properties
- A program used to document the CMOS System Time and Date on a computer seized as evidence
- A text-search utility that can scan DOS and Windows systems and locate targeted keywords and/or strings of text in computer-related investigations and computer security reviews
- A forensic binary data search tool that is used to identify targeted graphics file content and/or foreign language words and phrases stored in the form of computer data
- A utility that displays any network shares including local and remote
- A monitoring tool that displays logons, logoffs, and privilege usage

Selecting Incident Response/Forensic Tools

- Command-line tools are best; avoid tools that use a Windows (GUI) interface.
- Create several floppy disks containing your most important data collection tools.
- Use tested tools that you know work.

Incident Containment and Eradication of Vulnerabilities

- Contain the incident. The goal is to limit the scope and magnitude of an incident to prevent the incident from causing more damage.
- Determine the risk of continuing operations. If the system contains classified or sensitive information or if critical programs risk becoming corrupted, it is generally advised that the system be shut down or at least temporarily disconnected from the network.
- Sever network and Internet connections. For example, if a serious virus is suspected, such as a fast-spreading worm or dangerous Trojan horse, you should immediately disconnect the infected computer from the network.
- Understand the risks of using network and file shares. Many viruses and worms will use network file shares as a means to propagate across a network.
- Establish a trust model. A trust model is a means for helping to recognize and visualize varying degrees of confidence, intentionally or unintentionally granted to individuals, based upon the risks associated with granting confidence.
- Periodically change passwords. Passwords are one of the first lines of defense that users have to protect their systems. Changing them frequently or after a system compromise is mandatory.
- Promote security awareness by using multimedia documentation strategies that can be easily or periodically distributed to all organizational members.

Maintaining Chain-of-Custody Notes

- Use a notebook that does not permit any pages to be removed.
- Keep notes on the evidence found, which will go into your final report in more detail. These would essentially be notes that anyone could pick up and, at a glance, know exactly where you left off in your assessment of the seized computer and media.
- List the names of all personnel involved in the investigation including administrators responsible for the routine maintenance of systems.
- Include the current date and time (as well as appropriate time zone) for everything documented.
- Document broken hardware or any significant problems.
- Document special techniques (for example, sniffers, password crackers, and so on) used above and beyond normal processes.
- List outside sources used (for example, third-party companies or products that helped to provide assistance and information).
- Maintain a record of all applications running on the suspect's computer.
- Include a list of who had access to the collected evidence including date and time of access, as well as the date and time of any actions taken by those with access.
- Document the details of the initial assessment leading to the formal investigation.
- Specify the circumstances surrounding the suspected incident including who initially reported the suspected incident along with date and time.
- Maintain a complete list of all computer systems included in the investigation along with system specifications.
- Include a printed copy of any organizational policies and logon banners that relate to accessing and using computer systems.
- Keep a comprehensive list of steps used to collect and analyze evidence.

Disaster Recovery and Follow-Up

- Develop a Disaster Recovery Plan. Knowing how to react properly in an emergency is critical to making decisions that will minimize resultant damage and quickly restore operations.
- Develop incident recordkeeping procedures. The methods used to create your records are to be documented to ensure the ability to retrieve, read, and use those records in the future.
- Utilize an Uninterruptible Power Supply (UPS). In the event of a power failure, a generator may not supply the uninterrupted power required to maintain your computer system operation or to perform an orderly shutdown of a workstation or server.
- Perform regular backups. When disaster strikes, a backup may be the only hope of retrieving original data.
- After an incident, monitor systems for unusual or suspicious activity. In addition, a *post-mortem* examination should be conducted so that the organization can learn from the experience and, if necessary, update its procedures.
- Anticipate and plan for future attacks. Properly anticipating and planning for unforeseen disruptions to business operations is important for remaining competitive.

The Goals of a Disaster Recovery Plan

- Identify flaws and vulnerabilities and implement a disaster prevention program.
- Minimize disruptions to business operations.
- Facilitate recovery tasks.
- Reduce the complexity of the recovery effort.

Developing a Disaster Recovery Plan

- Provide management with an understanding of all the resources needed to develop and maintain an effective disaster recovery plan. In addition, the organization should have the committed support from all group members (for example, management or IT personnel) to help support and participate in the effort.
- Assemble an incident response team that includes representatives from every key division of the organization.
- Define recovery requirements from the perspective of business functions.
- Identify the risks. Every risk must be identified along with what steps would be necessary to thwart it happening in the first place.
- Document the impact of an extended loss to operations and key business functions. It is impossible for a disaster recovery plan to justify each expense included in every business process and application in the recovery process. The organization should therefore inventory and prioritize critical business processes.
- Select recovery teams to oversee the disaster recovery process and ensure that the required proper balance is maintained for disaster recovery plan development.
- Develop a contingency plan that is understandable, easy to use, and easy to maintain by all organization members.
- Define how contingency planning considerations are to be incorporated in your ongoing business planning. System development procedures must also be defined in order for the plans to remain viable.

Restoring the System

- Restore the system after compromise. Once a compromise has been eradicated, the next logical step is to restore the system to its fully operational state.
- Validate the system. Once the system has been restored, verify that the operation was successful and the system is back to its normal operating condition.
- Decide when to restore operations. Management may decide to leave the system offline while operating system upgrades and patches are installed.
- Monitor the systems. Once the system is back online, continue to monitor for backdoors that may have eluded detection.

Disaster Recovery Plan Training Goals for Employees

- Make employees aware of the need for a disaster recovery/business resumption plan.
- Inform all employees of the existence of the plan and provide procedures to follow in the event of an emergency.
- Train all personnel with responsibilities identified in the plan to perform the disaster recovery and business continuity procedures.
- Provide the opportunity for recovery teams to practice their disaster recovery and business continuity skills.

Implementing and Maintaining an Effective Records Security Program

- Ensure that only authorized personnel have access to electronic records.
- Provide for backup and recovery of records to protect against information loss.
- Ensure that appropriate personnel are trained to protect sensitive or classified electronic records.
- Minimize the risk of unauthorized alteration or erasure of electronic records.
- Ensure that electronic records security is included in your organization's overall information security plans.

Authentication Methods for Electronic Records

- A hard copy of a document accompanies the electronic media containing information about the electronic record that can be used for identifying, retrieving, or indexing.
- Attach an authentication label to the media.
- Link a digital signature to the electronic file or document.

Procedures to Improve the Legal Admissibility of Electronic Records as Evidence

- Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.
- Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure system protection against such problems as power interruptions.
- Identify the electronic media on which records are stored throughout their life cycle, and the maximum time that records remain on each type of storage medium.
- Coordinate all of the foregoing with appropriate senior management staff and legal counsel.

Creating a Backup Plan

- Designate one person as coordinator and record keeper of all backups.
- Put the plan in writing and keep it with the organization's security policies and procedures documentation.
- Include the name of the backup coordinator and/or record keeper in the plan.
- Include the type of data requiring backup in the plan.
- State the frequency of data backups in the plan.
- Cite the location of on-site data storage in the plan.
- Cite the location of offsite data storage in the plan.
- State the method used for backing up data along with a checklist of procedures in the plan.

Post-Incident Monitoring and Analysis

- Validate that the attack has subsided.
- Examine files and logs for details of the attack.
- Determine if legal action is warranted or possible.
- Reevaluate or modify overall computer network security.

Incident Postmortem Questions

- How did the incident start?
- Which vulnerabilities or flaws were exploited?
- How was access gained?
- How did the organization become aware of the incident?
- How was the incident eventually resolved?
- Were existing incident response procedures adequate or did they require updating?

Removing a Hacker from the System

- Kill all active or running processes that the hacker is using and remove any files or programs that he or she may have left on the system.
- Change passwords on any accounts accessed by the hacker/cracker and be sure to keep a log of all actions taken.
- Restore the system to a normal state, and restore any data or files that the hacker/cracker may have modified.
- Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Also, install patches for other vulnerabilities of which the hacker may not have taken advantage, and inform the appropriate people.
- All actions taken to restore the system to a normal state should be documented in the logbook for this incident.
- Once the incident has been contained and the hacker removed from the system, the next step is to contact the appropriate authorities.
- After the investigation is complete, a report describing the incident should be written and distributed to all incident response and security personnel.

Network Security Audit Elements

- Assessment of current security policies, procedures, and practices
- A vulnerability assessment
- Penetration testing
- Visual inspection of the network's physical security

Computer Security Policy Goals

- Establish policies to protect your organization's networks and computer systems from abuse and inappropriate use.
- Establish methods that will aid in the identification and prevention of abuse of the organization's networks and computer systems.
- Provide an effective method for responding to questions and complaints regarding abuses—real or unconfirmed—of the organization's networks and computer system.
- Establish procedures that will protect your professional reputation while allowing you to meet the organization's responsibilities (legal and ethical) regarding the computer system's Internet connection.

Security Policy Assessment Elements

- An explanation of the reason for the policy
- The effective date of the policy as well as the date it expires
- A listing of those who: (a) authorized the policy, (b) constructed the policy, (c) approved the policy, (d) will maintain the policy, and (e) will enforce the policy
- A listing of the personnel and staff that will be affected by the policy
- An outline of the actions the organization expects of its users
- The methods that will be used to enforce the policy
- The regulations and laws upon which the policy is based (including the in-house regulations of your organization)
- Which information assets must be protected
- The methods and procedures that personnel are to follow for reporting security violations (whether real or unsubstantiated)

The Basic Six-Step Computer Security Audit Process

- Analysis of vulnerabilities.** Determine the adequacy of your organization's security measures, identify security deficiencies, and evaluate the effectiveness of your existing security measures. The analysis should include the risk and likelihood of malicious coders, hackers, and insiders exploiting these flaws.
- Network assessment and infrastructure analysis.** Examine hardware devices, intrusion detection systems, routers, and firewalls for vulnerabilities that could leave you open to intrusions.
- Risk assessment.** List the safeguards you already have in place for protecting against potential threats by assessing their relative significance in terms of potential loss for all areas of your system. The results from this assessment can be used to determine which areas need the most attention first.
- Access and policy assessment.** Examine each user's availability and access to computer system resources. Be sure to include a review of password policies, backup policies, Internet access policy, network security policy, remote access policy, desktop policy, server platform policy, application security policy, personal Internet-based accounts, and in general, the guidelines for the development and implementation of policy standards throughout your organization.
- Physical security.** Examine physical computer assets for protection from vandalism, unauthorized access, and tampering. Include a review of all the organization's computer hardware and associated equipment, such as workstations, servers, terminals, routers, switches, removable storage media, hard copies of documentation, and support facilities.
- Findings and recommendations report.** Include all of the findings resulting from the analysis and assessments performed as well as recommendations for implementing countermeasures to any of the vulnerabilities discovered during the security audit.

Analyzing Workstations

When conducting your organization's computer network assessment, be sure to examine individual workstations for the following:

- Has the user enabled a workstation screen lock?
- Has a BIOS password been implemented?
- Is sensitive data stored on a workstation in a secure manner?
- Have all unused or unnecessary networking protocols been removed?
- Are unnecessary services, such as IIS (Microsoft's Internet Information Server), prevented from running on the workstation?
- Is virus protection installed, updated, and running?
- Are any unnecessary files and folders precluded from being shared on the workstation?
- Has the operating system been updated and patched against known vulnerabilities?
- Is there a procedure to automate the frequent backup of data?

Security Policy Audit Checklist Questions

- Have a broad range of employees within the organization—representative of a variety of positions and job levels—been involved in developing the security policy?
- Has the policy been drafted in a manner that can be understood and followed by all staff members?
- Has staff been informed of their security roles and responsibilities in writing?
- Have the needs and expectations of your organization been communicated to your personnel both initially and in an ongoing manner?
- Have your personnel received security training specifically tailored to the needs of their position?
- Are all new employees sufficiently trained regarding their security roles, responsibilities, and expectations?
- Are appropriate opportunities provided for personnel to voice security concerns and ask questions about security policies and procedures?
- Is adequate time provided for reading and reviewing security agreements before employees and outsiders are required to sign and submit them?
- Have your policy developers reviewed the policies (security-related practices) of other organizations in the same line of work or those with whom you will conduct business? Cooperation at this juncture ensures that all the engaged parties will be satisfied with future transactions.
- Has news of your organization's commitment to security been shared with the public?
- Have policy goals and objectives been translated into organizational security rules that are designed to modify staff behavior?
- Has an administrator been specifically appointed to be responsible for your organization's security?
- Are these security regulations enforced equally at all levels of your organization?
- Have security issues been included as a part of employee performance reviews?
- Are outsiders (for example, repair technicians and outside organizations) required to sign a contract acknowledging that they are aware of their responsibilities and that they will abide by your organization's security rules and regulations?
- Are security policies reviewed—and if need be, revised—at least on an annual basis?

Analyzing Network Servers

Be sure to also examine network servers for the following:

- Have the servers been located in a secure area that prevents unauthorized access?
- Has a BIOS password been implemented?
- Has all sensitive data been stored on an NTFS partition?
- Have all default accounts been disabled?
- Has the system administrator unbound unnecessary or unused protocols, such as IPX/SPX, NetBIOS, and so on?
- Have unnecessary services—such as SMTP, NTP, and FTP—been removed or disabled?
- Is virus protection software installed and regularly updated?
- Have any shared folders been given unique permissions for any individual users?
- Have service packs and security patches been installed when available?
- Is your network administrator on the organization's security mailing list (so as to be reminded to apply fixes and upgrades in a timely manner)?
- Are full backups made on a frequent, regular basis?
- Has your network administrator created and securely stored emergency repair disks?
- Has auditing and account logging been turned on?
- Are security event logs reviewed on a regular basis?
- Has the auto-run feature been disabled for CD-ROM use?
- Are audit logs being monitored?
- Has the server's real-time clock been synchronized to a central timeserver?
- Have password-cracking tools been used to detect weak or easily guessed passwords?
- Has a host-based intrusion detection system (IDS) been employed?
- Have floppy disk drives been disabled?
- Has auditing been enabled for the backup and restoration of data?
- Has anonymous logon been disabled or restricted?
- Have NetBIOS null sessions been disabled?
- Has the administrator account been renamed?
- If appropriate, has the SAM password database been encrypted with 128-bit encryption? (Use syskey.exe for NT4.0.)
- Have procedures and guidelines been established for responding to incidents?

Security Policy Mistakes to Avoid

- Installing unnecessary programs and services
- Opening e-mail message attachments from unknown people
- Not keeping current on software patches, especially security-related ones
- Not installing antivirus software and keeping its virus patterns current
- Lack of adequate training to administer the system
- Not deploying encryption or intrusion detection systems
- Inadequate handling of sensitive data
- Sharing passwords or using weak passwords
- Propagating chain mail and virus hoaxes

Information Security Precautions

- Protect your computer equipment. Keep it in a secure environment. Be sure to keep food, drink, and cigarette smoke away from it at all times. In addition, know where fire suppression equipment is located, and learn how to use it.
- Protect your area. Keep unauthorized people away from sensitive computer equipment and information and remember to question any strangers in your area.
- Protect your password. Never write it down or give it to anyone. In addition, do not use names, numbers, or dates that can be personally identified with you. Remember not only to change it often, but also to change it immediately if you think it has been compromised.
- Protect your files. Don't allow unauthorized access to your files and data, and remember to *never* leave your equipment unattended with your password activated; always sign off!
- Protect against malicious code. Don't use unauthorized software, and back up your critical files before implementing *any* new software.
- Lock up storage media that contains sensitive data. If the data or information is sensitive or critical to your organization, always be sure to lock it up in a secure location.
- Back up your data. Keep duplicates of your sensitive data in a safe place, out of your immediate area, and remember to back up data as often as necessary.
- Report security violations. Tell your system administrator or network security manager if you see any unauthorized changes to your data. Immediately report any loss of data or programs, whether automated or hard copy.