2000 CERT Tech Tip: Steps for Recovering from a UNIX or NT System Compromise

Original publication date: April 17, 2000

This document is being published jointly by the CERT Coordination Center and AusCERT (Australian Computer Emergency Response Team). It describes suggested steps for responding to a UNIX or NT system compromise. Your response should be carried out in several stages:

Introduction

This document sets out suggested steps for responding to a UNIX or NT system compromise.

Note that all actions taken during your recovery from a system compromise should be in accordance with your organization's policies and procedures.

1. Before you get started
    a. Consult your security policy

    a. If you do not have a security policy
        i. Consult with management

        Depending on how your organization is structured, it may be important to notify management in order to facilitate internal coordination of your recovery effort. Also be aware that intrusions may get the attention of the media.

        i. Consult with your legal counsel

        Before you get started in your recovery, your organization needs to decide if pursuing a legal investigation is an option.

        Note that the CERT Coordination Center and AusCERT (Australian Computer Emergency Response Team) are involved in providing technical assistance and facilitating communications in response to computer security incidents involving hosts on the Internet. We do not have legal expertise and cannot offer legal advice or opinions. For legal advice, we recommend that you consult with your legal counsel. Your legal counsel can provide you with legal options (both civil and criminal) and courses of action based on you or your organization's needs.

        It is up to you how you wish to pursue this incident. You may wish to secure your systems or to contact law enforcement to investigate the case.

        If you are interested in determining the identity of or pursuing action against the intruder, we suggest that you consult your management and legal counsel to see if any local, state, or federal laws have been violated. Based on that, you could then choose to contact a law enforcement agency and see if they wish to pursue an investigation.

        We encourage you to discuss the root compromise activity with your management and legal counsel to answer the following questions:

        - What is your legal status in terms of your ability to trap intruders or trace connections (i.e., do you have a login banner stating that connections can be tracked or traced? See CERT Advisory CA-1992-19, "Keystroke Logging Banner").
        - What are your legal responsibilities if your site is aware of the activity and does not take steps to prevent it?
        - Have any local, state, or federal laws been violated?
        - Should an investigation be pursued?
        - Should you report the activity to local, state, or national) law enforcement?

        i. Contact law enforcement agencies

        In general, if you are interested in pursuing any type of investigation or legal prosecution, we'd encourage you to first discuss the activity with your organization's management and legal counsel and to notify any appropriate law enforcement agencies (in accordance with any policies or guidelines at your site).

        Keep in mind that unless one of the parties involved contacts law enforcement, any efforts to trap or trace the intruder may be to no avail. We suggest you contact law enforcement before attempting to set a trap or tracing an intruder.

        U.S. sites interested in an investigation can contact their local Federal Bureau of Investigation (FBI) field office. To find contact information for your local FBI field office, please consult your local telephone directory or see the FBI's field offices web page available at:

            http://www.fbi.gov/contact/fo/fo.htm

        U.S. sites and foreign locations involving U.S. assets, interested in an investigation can contact their local U.S. Secret Service (USSS) Field Office. To find contact information for your local USSS Field Office, please consult your local telephone directory or see the USSS web site available at:

            http://www.secretservice.gov/field_offices.shtml

        To contact the USSS Electronic Crimes Branch please call:

            Phone: +1(202)406-5850
            Fax: +1(202)406-9233

        If your site involves a **Department of Defense** Contractor, a Department of Defense Entity or any of the U.S. Military Services, and you are interested in an investigation, you may contact the United States Department of **Defense Criminal Investigative Service** (DCIS), Pittburgh, Pennsylvania at telephone number +1(412)395-6931. For information regarding DCIS please see:

            http://www.dodig.osd.mil/INV/DCIS/programs.htm

        Non-U.S. sites may want to discuss the activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

        To contact the Australian Federal Police:

Canberra	+61 2 6256 7777	Ask for the Co-ordination centre

Brisbane	+61 7 3222 1222	Ask for Operations
Sydney	+61 2 9286 4000	Ask for the Co-ordination centre
Melbourne	+61 3 9607 7777	Ask for the Co-ordination centre
Adelaide	+61 8 8419 1811	Ask for the Co-ordination centre
Perth	+61 8 9320 3444	Ask for the Co-ordination centre
Darwin	+61 8 8981 1044	Ask for the Co-ordinator

ii. Notify others within your organization

In addition to notifying management and legal counsel at your site, you may also need to notify others within your organization who may be directly affected by your recovery process (e.g., other administrators or users).

a. Document all of the steps you take in recovering
The importance of documenting every step you take in recovery can not be overstated. Recovering from a system compromise can be a hectic and time-consuming process and hasty decisions are often made. Documenting the steps you take in recovery will help prevent hasty decisions and give you a record of all the steps you took to recover, which you can reference in the future. Documenting the steps you take in recovery also may be useful if there is a legal investigation.

1. Regain control
   a. Disconnect compromised system(s) from the network
   To regain control, you will need to disconnect all compromised machines from your network including dial in connections. After that you may wish to operate in single user mode in UNIX or as the local administrator in NT to ensure that you have complete control of the machine; however, by rebooting or changing to single user/local administrator mode, you may lose some useful information because all processes executing at the time of discovery will be killed.

   Therefore, you may wish to work through steps in section C.5. Look for signs of a network sniffer to determine if the compromised system is currently running a network sniffer.

   Operating in single user mode on UNIX systems will prevent users, intruders, and intruder processes from accessing or changing state on the compromised machine while you are going through the recovery process.

   If you do not disconnect the compromised machine from the network, you run the risk that the intruder may be connected to your machine and may be undoing your steps as you try to recover the machine.

   a. Copy an image of the compromised system(s)
   Before analyzing the intrusion we encourage you to create a backup of your system. This will provide a "snapshot" of the file system at the time that the root compromise was first discovered. You may need to refer back to this backup in the future.

   If you have an available disk which is the same size and model as the disk in the compromised system, you can use the ***dd*** command in UNIX to make an exact copy of the compromised system.

   For example, on a Linux system with two SCSI disks, the following command would make an exact replica of the compromised system (/dev/sda) to the disk of the same size and model (/dev/sdb).

```
# dd if=/dev/sda of=/dev/sdb
```

   Please read the ***dd*** man page for more information.

   There are many other ways to create a backup of your system. On NT systems there is no built in command like *dd*, but there are a number of third party applications that will make an image copy of an entire hard drive.

   Creating a low level backup is important in case you ever need to restore the state of the compromised machine when it was first discovered. Also, files may be needed for a legal investigation. Label, sign, and date the backup and keep the backup in a secure location to maintain integrity of the data.

1. Analyze the intrusion
   With your system disconnected from the network, you can now thoroughly review log files and configuration files for signs of intrusion, intruder modifications, and configuration weaknesses.

   a. Look for modifications made to system software and configuration files
   Verify all system binaries and configuration files.

   When looking for modifications of system software and configuration files, keep in mind that any tool you are using on the compromised system to verify the integrity of binaries and configuration files could itself be modified. Also keep in mind that the kernel (operating system) itself could be modified. Because of this, we encourage you to boot from a trusted kernel and obtain a known clean copy of any tool you intend to use in analyzing the intrusion. On UNIX systems you can create a boot disk and make it write protected to obtain a trustworth kernel.

We urge you to check all of your system binaries thoroughly against distribution media. We have seen an extensive range of Trojan horse binaries that have been installed by intruders.

Some of the binaries which are commonly replaced by Trojan horses on UNIX systems are: telnet, in.telnetd, login, su, ftp, ls, ps, netstat, ifconfig, find, du, df, libc, sync, inetd, and syslogd. Also check any binaries referenced in /etc/inetd.conf, critical network and system programs, and shared object libraries.

On NT systems, Trojan horses commonly introduce computer viruses or "remote administration" programs such as Back Orifice and NetBus. There have been cases where the system file that handles internet connectivity was replaced with a Trojan horse.

Because some Trojan horse programs could have the same timestamps as the original binaries and give the correct ***sum*** values, we recommend you use ***cmp*** on UNIX systems to make a direct comparison of the binaries and the original distribution media.

Alternatively, you can check the MD5 results for either UNIX or NT on suspect binaries against a list of MD5 checksums from known good binaries. Ask your vendor if they make MD5 checksums available for their distribution binaries.

Additionally, verify your configuration files against copies that you know to be unchanged.

When inspecting your configuration files on UNIX systems, you may want to

- check your /etc/passwd file for entries that do not belong.
- check to see if /etc/inetd.conf has been modified.
- if you allow the "r-commands" (rlogin, rsh, rexec), ensure that there is nothing that does not belong in /etc/hosts.equiv or in any .rhosts files.
- check for new SUID and SGID files. The following command will print out all SUID and SGID files within your filesystem.

```
# find / \( -perm -004000 -o -perm -002000 \) -type f -print
```

When inspecting NT systems, you may want to

- check for odd users or group memberships.
- check for changes to registry entries that start programs at logon or services. (see **LISTING 1**)
- check for unauthorized hidden shares with the 'net share' command or Server Manager tool.
- check for processes that you do not identify using the pulist.exe tool from the NT resource kit or the NT Task Manager.

a. Look for modifications to data
Data on compromised systems is often modified by intruders. We encourage you to verify the integrity of web pages, ftp archives, files in users' home directories, and any other data files on your system.

a. Look for tools and data left behind by the intruder
Intruders will commonly install custom-made tools for continued monitoring or for access to a compromised system.

The common classes of files left behind by intruders are

- **Network Sniffers**

  A network sniffer is a utility which will monitor and log network activity to a file. Intruders commonly use network sniffers to capture username and password data that is passed in cleartext over the network. (see section C.5 below)

  Sniffers are more common on UNIX systems, but on NT systems check for key logging programs.

- **Trojan Horse Programs**

  Trojan horse programs are programs that appear to perform one function while actually performing a different function. Intruders use Trojan horse programs to hide their activity, capture username and password data, and create backdoors for future access to a compromised system. (see section C.1 above)

- **Backdoors**

  Backdoor programs are designed to hide itself inside a target host. The backdoor allows the user that installed it to access the system without using normal authorization or vulnerability exploitation.

- **Vulnerability Exploits**

  A majority of compromises are a result of machines running vulnerable versions of software. Intruders often use tools to exploit known vulnerabilities and gain unauthorized access. These tools are often left behind on the system in "hidden" directories.

- **Other Intruder Tools**

  The intruder tools listed above are not intended to be a conclusive or comprehensive list. There may be other tools left behind by an intruder. Some of the other types of tools you may find are tools to
  - probe systems for vulnerabilities
  - launch widespread probes of many other sites
  - launch denial of service attacks
  - use your computing and networking resources

- **Intruder Tool Output**

You may find log files from any number of intruder tools. These log files may contain information about other sites involved, vulnerabilities of your compromised machine(s), and vulnerabilities at other sites.

We encourage you to search thoroughly for such tools and output files. Be sure to use a known clean copy of any tool that you use to search for intruder tools.

When searching for intruder tools on a compromised system

- Look for unexpected ASCII files in the /dev directory on UNIX systems. Some of the Trojan binaries rely on configuration files which are often found in /dev.
- Look very carefully for hidden files or directories. If an intruder has created a new account and home directory then there may be hidden files or directories.
- Look for files or directories with strange names such as "..." (three dots) or ".. " (two dots and some whitespace) [UNIX]. Intruders often try and hide files within such directories. On NT systems, look for files and directories that closely match what may appear as a system file (EXPLORE.EXE, UMGR32.EXE, etc).

a. Review log files
Reviewing your log files will help you get a better idea of how your machine was compromised, what happened during the compromise, and what remote hosts accessed your machine.

Keep in mind when reviewing any log files from a compromised machine that any of the logs could have been modified by the intruder.

On UNIX systems, you may need to look in your /etc/syslog.conf file to find where syslog is logging messages. NT systems generally log everything to one of three logs for NT events, all of which are viewed through the Event Viewer. Other NT applications such as IIS server may log to other locations. IIS by default writes logs to the c:\winnt\system32\logfiles directory.

Below is a list of some of the more common UNIX log file names, their function, and what to look for in those files. Depending on how your system is configured, you may or may not have the following log files.

- **messages**

  The **messages** log will contain a wide variety of information. Look for anomalies in this file. Anything out of the ordinary should be inspected. Also, look for events that occurred around the known time of the intrusion.

- **xferlog**

  If the compromised system has a functioning ftp server, **xferlog** will contain log files for all of the ftp transfers. This may help you discover what intruder tools have been uploaded to your system, as well as what information has been downloaded from your system.

- **utmp**

  This file contains binary information for every user currently logged in. This file is only useful to determine who is currently logged in. One way to access this data is the ***who*** command.

- **wtmp**

  Every time a user successfully logs in, logs out, or your machine reboots, the wtmp file is modified. This is a binary file; thus, you need to use a tool to obtain useful information from this file. One such tool is ***last***. The output from ***last*** will contain a table which associates user names with login times and the host name where the connection originated. Checking this file for suspicious connections (e.g., from unauthorized hosts) may be useful in determining other hosts that may have been involved and finding what accounts on your system may have been compromised.

- **secure**

  Some versions of UNIX (RedHat Linux for example) log tcp wrapper messages to the **secure** log file. Every time a connection is established with one of the services running out of inetd that uses tcp wrappers, a log message is appended to this log file. When looking through this log file, look for anomalies such as services that were accessed that are not commonly used, or for connections from unfamiliar hosts.

The common item to look for when reviewing log files is anything that appears out of the ordinary.

a. Look for signs of a network sniffer
When a system compromise occurs, intruders could potentially install a network monitoring program on UNIX systems, commonly called a sniffer (or packet sniffer), to capture user account and password information. For NT systems, remote administration programs would be more commonly used for the same purpose.

The first step to take in determining if a sniffer is installed on your system is to see if any process currently has any of your network interfaces in promiscuous mode. If any interface is in promiscuous mode, then a sniffer could be installed on your system. Note that detecting promiscuous interfaces will not be possible if you have rebooted your machine or are operating in single user mode since your discovery of this intrusion.

There are a couple of tools designed for this purpose.

- **cpm** - UNIX

  available for download from:

ftp://coast.cs.purdue.edu/pub/tools/unix/sysutils/cpm/

- **ifstatus** - UNIX

  available for download from:

  ftp://coast.cs.purdue.edu/pub/tools/unix/sysutils/ifstatus/

Keep in mind that some legitimate network monitors and protocol analyzers will set a network interface in promiscuous mode. Detecting an interface in promiscuous mode does not necessarily mean that an intruder's sniffer is running on a system.

Another issue to consider is that sniffer log files tend to grow quickly in size. You may want to use utilities such as ***df*** to determine if part of the filesystem is larger than expected. Remember that ***df*** is often replaced by a Trojan horse program when sniffers are installed; therefore, be sure to obtain a known clean copy of that utility if you do use it.

If you find that a packet sniffer has been installed on your systems, we strongly urge you to examine the output file from the sniffer to determine what other machines are at risk. Machines at risk are those that appear in the destination field of a captured packet, but if passwords across systems are common or if the source and destination machines trust each other the source machine will also be at further risk.

Many common sniffers will log each connection as follows:

```
-- TCP/IP LOG -- TM: Tue Nov 15 15:12:29 --
PATH: not_at_risk.domain.com(1567) => at_risk.domain.com(telnet)
```

For sniffer logs of this particular format, you can obtain a list of affected machines by executing the following command:

```
% grep PATH: $sniffer_log_file | awk '{print $4}' | \
  awk -F\( '{print $1}'| sort -u
```

You may need to adjust the command for your particular case. Also, some sniffers encrypt their logs so they may not be obvious. Because of this check for files that grow quickly.

You should be aware that there may be other machines at risk in addition to the ones that appear in the sniffer log. This may be because the intruder has obtained previous sniffer logs from your systems or through other attack methods.

For more information, we encourage you to review CERT Advisory CA-1994-01, available from:

http://www.cert.org/advisories/CA-1994-01.html

The advisory describes of sniffer activity and suggests approaches for addressing this problem.

Please send us a list of all hosts you know to be affected. This will help us determine the scope of the problem.

If Australian or New Zealand hosts have been involved, please inform auscert@auscert.org.au.

a. Check other systems on your network
   We encourage you to check all of your systems, not just those that you know to be compromised. In your check include any systems associated with the compromised system through shared network-based services (such as NIS and NFS) or through any method of trust (such as systems in hosts.equiv or .rhosts files, or a Kerberos server).

   In examining other systems on your network, we encourage you to use our Intruder Detection Checklists:

   http://www.cert.org/tech_tips/intruder_detection_checklist.html
   http://www.cert.org/tech_tips/win_intruder_detection_checklist.html

a. Check for systems involved or affected at remote sites
   While examining log files, intruder output files, and any files modified or created during and since the time of the intrusion, look for information that leads you to suspect that another site may be linked with the compromise. We often find that other sites linked to a compromise (whether upstream or downstream of the compromise) have often themselves been victims of a compromise. Therefore it is important that any other potential victim sites are identified and notified as soon as possible.

1. Contact the relevant CSIRT and other sites involved
   a. Incident Reporting
      Intruders will frequently use compromised accounts or hosts to launch attacks against other sites. If you find evidence of compromise or intruder activity at any other sites, we encourage you to contact those sites. Tell them what you have found, explain that this may be a sign of compromise or intruder activity at their site, and suggest that they may wish to take steps to determine if/how the compromise occurred and prevent a recurrence. When contacting other sites, please give them as much detail as possible including date/timestamps, timezone, and what to do if they have follow-up information.

      We would appreciate a "cc" to cert@cert.org or auscert@auscert.org.au as appropriate on any correspondence. If you like, you can let the site know that you are working with us on this incident (please include the assigned CERT or AusCERT tracking number in the subject line of your messages). Also let them know that we can offer assistance on how to recover from the compromise.

   a. Contact AusCERT - Australian Computer Emergency Response Team

We would appreciate it to be informed of any incidents involving Australian and New Zealand sites as it helps us to gauge the extent and nature of intruder activity.

Our contact information is as follows:

Internet: auscert@auscert.org.au *monitored during business hours (GMT+10:00)*
Telephone: +61 7 3365 4417 *monitored during business hours (GMT+10:00)*
Hotline: +61 7 3365 4417 *monitored 24 hours, 7 days for emergencies (GMT+10:00)*
Facsimile: +61 7 3365 7031

Australian Computer Emergency Response Team
The University of Queensland
Brisbane
Qld 4072
AUSTRALIA

a. Contact the CERT Coordination Center
We would appreciate it if you would complete and return an Incident Reporting Form as this will help us better assist you, and allow us to relate ongoing intruder activities. This also provides us a better overview of trends in attack profiles and provides input for other CERT documents such as Advisories. We prefer that Incident Reporting Forms are sent to us via email. The Incident Reporting Forms are available from:

http://www.cert.org/reporting/incident_form.txt

Our contact information is as follows:

Email: cert@cert.org (monitored during business hours)
Telephone: +1-412-268-7090 24-hour hotline
Fax: +1-412-268-6989
CERT Coordination Center personnel answer business days (Monday-Friday) 08:30-17:00 EST/EDT (GMT-5) /(GMT-4), on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA USA 15213-3890

a. Obtain contact information for other sites involved
If you need contact information for a .COM, .EDU, .NET, or .ORG top-level domain, we encourage you to use the InterNIC's whois database.

http://www.internic.net/whois.html

To find contact information from the appropriate registrar, we encourage you to use the InterNIC's Registrar Directory:

http://www.internic.net/origin.html

To find contact information for the Asia-pacific region and Australia respectively:

http://www.apnic.net/apnic-bin/whois.pl

http://www.aunic.net/cgi-bin/whois.aunic

To find contact information for other incident response teams, you may also want to check the contact list of the Forum of Incident Response and Security Teams (FIRST), available in:

http://www.first.org/team-info/

More information about finding site contacts is available from:

http://www.cert.org/tech_tips/finding_site_contacts.html

We do not recommend sending email to "root" or "postmaster" of a machine that is suspected of being involved in intruder activity. If that machine is the source of an intruder attack, it is possible that that machine itself may be compromised and the intruder may have root access and/or be reading or intercepting email sent to that host.

If you are still unsure of a site or contact details, please get in touch with us.

a. Recover from the intrusion
   i. Install a clean version of your operating system
   Keep in mind that if a machine is compromised, anything on that system could have been modified, including the kernel, binaries, datafiles, running processes, and memory. In general, the only way to trust that a machine is free from backdoors and intruder modifications is to reinstall the operating system from the

distribution media and install all of the security patches before connecting back to the network. Merely determining and fixing the vulnerability that was used to initially compromise this machine may not be enough.

We encourage you to restore your system using known clean binaries. In order to put the machine into a known state, you should re-install the operating system using the original distribution media.

i. Disable unnecessary services
Configure your system to offer only the services that the system is intended to offer and no others. Check to ensure that there are no weaknesses in the configuration files for those services and that those services are available only to the intended set of other systems. In general, the most conservative policy is to start by disabling everything and only enabling services as they are needed.

i. Install all vendor security patches
We strongly encourage you to ensure that the full set of security patches for each of your systems is applied. This is a major step in defending your systems from attack and its importance cannot be overstated.

We encourage you to check with your vendor regularly for any updates or new patches that relate to your systems.

i. Consult AusCERT advisories and external security bulletins
We encourage you to consult past AusCERT advisories and external security bulletins and to follow the instructions that are relevant to your particular configuration. Be sure that you have installed all applicable patches or workarounds described in the AusCERT publications.

Remember to check the advisories periodically to ensure that you have the most current information.

Past AusCERT advisories are available from:

http://www.auscert.org.au/Information/Advisories/aus_advisories.html
ftp://ftp.auscert.org.au/pub/auscert/advisory/

External Security Bulletins are available from:

http://www.auscert.org.au/Information/Advisories/esb_advisories.html
ftp://ftp.auscert.org.au/pub/auscert/ESB/

i. Consult CERT advisories
We encourage you to consult past CERT advisories and to follow the instructions that are relevant to your particular configuration. Be sure that you have installed all applicable patches or workarounds described in the CERT publications.

Remember to check the advisories periodically to ensure that you have the most current information.

Past CERT advisories are available from:

http://www.cert.org/advisories/

i. Caution use of data from backups
When restoring data from a backup, ensure that the backup itself is from an uncompromised machine. Keep in mind that you could re-introduce a vulnerability that would allow an intruder to gain unauthorized access. Also, if you are only restoring users' home directories and data files, keep in mind that any of those files could contain Trojan horse programs. You may want to pay close attention to .rhosts files in users' home directories.

i. Change passwords
After all security holes or configuration problems have been patched or corrected, we suggest that you change the passwords of **ALL** accounts on the affected system(s). Ensure that passwords for all accounts are not easy to guess. You may want to consider using vendor-supplied or third-party tools to enforce your password policies.

AusCERT has published the Choosing good passwords article which contains information to educate users to choose good passwords.

a. Improve the security of your system and network
   i. Review security using the UNIX or NT Configuration Guidelines document
   To help you assess the security of your system(s), please refer to our UNIX or NT Configuration Guidelines documents. These documents may be useful when

checking your system for common configuration problems that are often exploited by intruders.

http://www.cert.org/tech_tips/unix_configuration_guidelines.html

http://www.cert.org/tech_tips/win_configuration_guidelines.html

i. Install security tools
Install all security tools before you connect your machine back to the network. Also, this is a good time to take an MD5 checksum snapshot of the newly restored system using a tool such as Tripwire®.

i. Enable maximal logging
Make sure that logging/auditing/accounting programs are enabled (for example, process accounting) and that they are set to an appropriate level (for example, sendmail logging should be level 9 or higher). Backup your logs and/or consider writing your logs to a different machine, to an append-only file system, or to a secure logging host.

i. Configure firewalls to defend networks
Consider filtering certain TCP/IP services at your firewall server, router or at the hosts. For some suggestions, please refer to "Packet Filtering for Firewall Systems," available from

http://www.cert.org/tech_tips/packet_filtering.html

a. Reconnect to the Internet
If you disconnected from the Internet, the best time to reconnect is after you have completed all the steps listed above.

a. Update your security policy
The CERT Coordination Center recommends that every site develop their own computer security policy. Each organization may have a specialized culture and security requirements that are specific to their own organization. Please refer to RFC 2196 "Site Security Handbook" for information about developing computer security policies and procedures for sites that have systems on the Internet. This document is available from

ftp://ftp.isi.edu/in-notes/rfc2196.txt

i. Document lessons learned from being compromised
Document and review the lessons you learned from going through the process of recovering from a compromise. This will help you decide exactly how to revise for your security policy.

i. Calculate the cost of this incident
For many organizations, changes simply are not made in security policy until they understand the cost of security, or lack thereof. Calculating the cost of an incident will help measure the importance of security for your organization. You may find that calculating the cost of this incident is useful for explaining to management that security is important to your organization.

i. Incorporate necessary changes (if any) in your security policy
Making changes to your security policy is the last step to take in this process. Be sure to inform members of your organization about the changes that have been made and how that may affect them.

Revision
History
April 17, 2000 Initial Release