INCIDENT RESPONSE PLAN
CATS - INFORMATION TECHNOLOGY

VERSION HISTORY

Version	Date	Author Name	Reason for Revision
1.1	6-24-2008	Michael Natale	Initial Publication - DRAFT
1.1	07-9-2010	Michael Natale	Annual Review
1.1	10-3-2011	Michael Persina	Annual Review
1.1	11-15-2012	Michael Persina	Annual Review – No Changes
1.1	4-9-2014	Ken Nelson	Annual Review
1.2	05-25-2015	Michael Natale	Annual Review
1.2	08-01-2016	Michael Natale	Annual Review
1.2	10-01-2017	Michael Natale	Annual Review
1.2	1-23-2020	John Remley	Annual Review
1.3	9-28-2021	John Remley	Annual Review and Updates
1.3	4-20-2022	Mike Natale	Annual Review and fixed bad link
1.3.1	5-1-2023	Mike Natale	Annual Review and fixed bad link
1.3.1	2/23/2024	Mike Natale	Annual Review

WRIGHT STATE UNIVERSITY	**Wright State University** Information Security	WRIGHT STATE UNIVERSITY

Controls	
Policy Title:	Incident Response Plan
Category:	Information Technology
Audience:	WSU Faculty, Staff, and Students
Reason for Revision:	*N/A*
Created / Modified Date:	6-24-08
Next Review Date:	2-1-2025
Location:	https://raidermailwright.sharepoint.com/sites/communities/organizations/cats/is/Information%20Security%20Policies/Forms/AllItems.aspx

Responsible Parties	
Author	Mike Persina
Technical Reviewer/Mgr	Mike Persina
Security Reviewer	John Remley

TABLE OF CONTENTS

Plan Purpose

Responding to computer security incidents, generally, is not a simple matter. Incident management and response activities require technical knowledge, communication, and coordination among personnel who respond to the incident.

Although incident management may vary in approach, depending on the situation, the goals are constant. Accordingly, the goals of this plan are:

- Helping affected entities recover quickly and efficiently from security incidents.
- Minimizing the impact due to the loss or theft of information or disruption of critical computing services when incidents occur.
- Responding, systematically, following proven procedures, which will dramatically decrease the likelihood of reoccurrence.
- Balancing the operational and security requirements within realistic budgetary constraints.

Report Incident:
http://www.wright.edu/security/incident

Computer Incident Response & Management Plan:
https://www.wright.edu/sites/www.wright.edu/files/page/attachments/incident-response-plan.pdf

1. Introduction

Identification of Document

This document is the computer incident response and management plan for the Computing and Telecommunications Services (CaTS) Department of Wright State University.

Purpose

The purpose of this document is to detail the computer incident response and management program for CaTS at Wright State University. Its intended usage is to guide those charged with mitigating computer incidents through the process of managing and successfully resolving a computer incident as well as documenting the incident as needed and notifying the appropriate parties about the incident.

Scope

This incident response and management plan establishes the protocol to be followed in the event of a computer security related incident at Wright State University. The recommend procedures incorporated into this document are comprised of industry best practices as represented by:

- The Computer Emergency Response Team (CERT) of the Software Engineering Institute of Carnegie Mellon University; and
- The SANS (System Administration, Networking, and Security) Institute, a cooperative research and education organization comprised of system administrators, security professionals, and network administrators.
- Educause, UNISOG, and other university security professionals.

Supporting Documents

- http://www.wright.edu/security/

Appendices

- Notification Chart as Appendix A.
- Linux Incident Response Checklist as Appendix B.
- Windows Incident Response Checklist as Appendix C.
- Mac Incident Response Checklist as Appendix D.
- Mobile Device Incident Response Checklist as Appendix E.
- Ransomware Playbook as Appendix F.

2. Background

Responding to computer security incidents, generally, is not a simple matter. Incident management and response activities require technical knowledge, communication, and coordination among personnel who respond to the incident.

Although incident management may vary in approach, depending on the situation, the goals are constant. Accordingly, the goals of this plan are:

- Helping affected entities recover quickly and efficiently from security incidents.
- Minimizing the impact due to the loss or theft of information or disruption of critical computing services when incidents occur.
- Responding, systematically, following proven procedures, that will dramatically decrease the likelihood of reoccurrence.
- Balancing the operational and security requirements within realistic budgetary constraints.

Definitions

The term **"incident"** refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event. Examples of incidents include:

- Unauthorized use of the system as a gateway to other systems.
- Unauthorized use of another user's account.
- Unauthorized use of a system.
- Execution of malicious code that destroys data.

Other adverse events include floods, fires, electrical outages, and excessive heat that cause system crashes. Adverse events such as natural disasters and power-related disruptions, though certainly undesirable incidents, are not generally within the scope of incident response and should be addressed in Wright State University's continuity (contingency) plan. For the purpose of *Incident Response*, therefore, the term "incident" refers to an adverse event that is related to Information Security.

An **"event"** is *any* observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash, and packet flooding within a network. Events sometimes provide an indication that an incident is occurring.

The term **"adequate security"** means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Incident Classification

The term "incident" encompasses the following general categories of adverse events as identified by the CaTS staff:

Problematic Email. Problematic email is characterized as email that is unwanted by the recipient and as such the recipient makes a formal complaint concerning the email. Examples of this are: hate mail, threatening letters, or persistent and unwanted romantic advances.

Account Misuse. Account misuse occurs when a user givens another person their user name and password. Account misuse is discovered when the username concurrently connects from two or more separate physical locations.

Account Compromise (non-privileged account). An account compromise occurs when a user's account is accessed using the correct user name and password but without the user knowingly having given their user name and password to another.

Account Compromise (privileged account). As previously stated an account compromise occurs when a user's account is accessed using the correct user name and password but without the user knowingly having given their user name and password to another. However, unlike the ordinary user who is non-privileged, the privileged account has control of system resources. Once a machine has been compromised at the privileged account level, it is highly susceptible to all known attacks.

Virus. A virus is software designed and written to adversely affect a computer by altering the way it works without the system owner's knowledge or permission. A benign virus is one that is designed to do no real damage to a computer. A malignant virus is one that attempts to inflict malicious damage to a computer.

Internal Attack. An internal attack is an attack that originates from a computer within the Wright State University domain and targets other computers within the Wright State University domain.

External Attack. An external attack is an attack that originates from a computer outside the Wright State University domain and targets computers within the Wright State University domain.

Outbound Attack. An outbound attack is one that originates inside of the Wright State University domain and targets computers outside of the Wright State University domain.

Other Theft and incidents not included in previous classifications.

The following are five examples of a computer attack:

1. Malicious code attacks. Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written to disguise its presence and is often difficult to detect. Self-replicating malicious code such as viruses and worms can replicate rapidly making containment an especially difficult problem.

2. Unauthorized access. Unauthorized access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to unauthorized access to files and directories stored on a system or storage media by obtaining superuser privileges. Unauthorized access could also entail access to network data by planting an unauthorized "sniffer" program or device to capture all packets traversing the network at a particular point.

3. Unauthorized utilization of services. It is not necessary to access another user's account to perpetrate an attack on a system or network. An intruder can access information, plant Trojan horse programs, and so forth by misusing available services. Examples include using the network file system (NFS) to mount the file system of a remote server machine or inter-domain access mechanisms in Windows to access files and directories in another organization's domain.

4. Disruption of service. Users rely on services provided by network and computing services. Perpetrators and malicious code can disrupt these services in many ways, including erasing a critical program, "mail

spamming" (flooding a user account with electronic mail), and altering system functionality by installing a Trojan horse program.

5. Password Cracking. An authorized or unauthorized user attempts to obtain the user names and passwords of legitimate users by employing some script or program.

6. Social Engineering.

3. Requisite Infrastructure

Planning is paramount to successful incident response and mitigation. In order for a system to be restored to its original state, that state must be known and recorded. Likewise, in order for system logs to be reviewed, logging functions must be enabled. Finally, in order for file comparisons to be made to detect if file alteration has occurred, the most recent copy of all system executables, or binaries, must be preserved.

In furtherance of security planning infrastructure CaTS has instituted the following infrastructure to both prevent an incident and in the event of an incident to facilitate successful incident mitigation:

- Intrusion detection has been implemented on critical systems.
- System logging functions are enabled and the actual logs should are placed well inside of the secure perimeter of the system.
- A password management program has been established that forces periodic change of passwords as well as enforcing rules to make selected passwords are less susceptible to attempts to guess or crack encrypted passwords.
- Unused recording media is available to make system backups and copies of files that have been altered. These copies are used for evidentiary purposes.
- System binaries and executables and copies of all configuration files for network devices have been archived.
- Login banners have been posted identifying ownership of the system whenever a user logs onto the Wright State University system.

In addition to the above, the following are recommended:

- Assign roles and responsibilities to IT personnel before an incident occurs to insure that they clearly understand what is required of them should an incident happen.
- Determine, in advance, who will be notified that an incident has occurred, and who is responsible for the overall coordination of the mitigation effort (usually the role of the IT security officer).
- Establish a mechanism to provide update or progress information that will not interfere with the personnel tasked to deal with the intrusion.
- Implement a trouble ticketing system to record, track and quantify incidents. The trouble ticketing system should be capable of generating a file or case number, be accessible to all that are assigned to resolve incidents, and be capable of receiving and filing of email messages

4. Incident Handling Procedures

The incident handling process consists of six steps:

- Initial Response – Identify whether or not an incident has occurred or is occurring. This process begins after someone notices some anomaly in the system or network.

- Intrusion Analysis – Determine the extent of the incident and contain it to prevent it from getting worse.
- System Repair – Make sure that the problem is eliminated.
- Security Improvement – Identify and eliminate the means by which the system was compromised.
- Network Reconnect - Restore the system to an operational status.
- Security Policy Update – Based upon any lessons learned from analysis of the incident update the security policy if needed

The following further details each of the six aforementioned steps. The recommended actions are predicated upon a worse case scenario – a root compromise. Incidents of lesser severity require a more limited response.

Initial Response

Compromises must be resolved as soon as possible, preferably the day of the notification. Compromised hosts must be reformatted, rebuilt and have vulnerabilities resolved before reconnecting them to the network. CaTS may decide, after review, that compromised hosts may be cleaned and patched expeditiously. Incidents must be resolved to the satisfaction of Cats before compromised hosts are reconnected to the network or filters are lifted. In some cases, CaTS may request privileged access to ensure the host is safe to resume network connectivity, or may require that it be evaluated for vulnerabilities before being placed back in service.

Initial Determination.

Determine whether the event is actually indicative of an incident and if so the type and severity of the incident.

Required Response.

Based upon the severity of the incident - attempt to determine the appropriate level of response required to mitigate the incident. Determine if the objective is solely to restore the system and prevent a re-occurrence, or will there be an effort to identify the perpetrator and file either a civil or a criminal action? If the intention is to pursue legal action then anything on the system may potentially be evidence and is subject to special requirements. If the objective is unknown then it must be assumed that a legal action could take place, therefore you must treat all files on the system as if they are evidence. If a loss of confidential information has occurred or is suspected contact the CaTS computer incident response team immediately.

Notification

Open a ticket in the incident reporting system and notify the designated party(s) responsible for initially responding to security incidents. Report an Incident

Identify contiguous systems and share information.

Keep key people in the loop, particularly administrators of adjacent or contiguous systems.

Isolate the affected system or systems from the rest of the network.

Regain control by disconnecting all compromised machines from the network.

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

Back-Up

Back up the affected system(s) to new unused media. Before analyzing the intrusion, 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. 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. Label, sign and date the backup and keep the backups in a secure location to maintain integrity of the data.

Avoid the Obvious

Avoid looking for the intruder with obvious methods like finger, ping or traceroute.

Identify all items that could possibly be considered as evidence.

Identify all times that have evidentiary value. Include computer printouts and logs that may have evidentiary value or be helpful in identifying the intruder.

Intrusion Analysis

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.
http://sans.org/resources/winsacheatsheet.pdf
http://www.sans.org/score/checklists/ID_Windows.pdf
http://www.sans.org/score/checklists/ID_Linux.pdf

Look for modifications made to system software and configuration files

Look for modifications to data

Look for tools and data left behind by the intruder

Intruders will commonly install custom-made tools for continued monitoring or access to a root compromised system.

The common classes of files left behind by intruders are as follows:

- **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 clear-text over the network.
- **Trojan Horse Programs**
  Trojan horse programs are programs that appear to function properly, but either add or remove features. Intruders use Trojan horse programs to hide their activity, capture username and password data, and create backdoors for future access to a root compromised system.
- **Vulnerability Exploits**
  The majorities of root compromises are a result of machines running vulnerable versions of software. Intruders often use tools to exploit known vulnerabilities and gain root access. These tools are often left behind on the system in "hidden" directories.
- **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.

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.

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 root compromised machine that any of the logs could have been modified by the intruder.

Look for signs of a network sniffer

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.

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.

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.

You may need to adjust the command for your particular case. 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.

Check other systems on your network

In examining other systems on your network, use the Intruder Detection Checklist in Appendix 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. It is therefore important that any other potential victim sites are identified and notified as soon as possible.

System Repair

Install a clean version of the operating system

Keep in mind that if a machine is compromised, anything on that system could have been modified, including the kernel, binaries, data files, 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 the machine may not be enough.

Disable unnecessary services

Ensure that your system is configured 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.

Install all vendor recommended security patches

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. Check with your vendor for any updates or new patches that relate to your systems.

Consult advisories, summaries, and vendor-initiated bulletins

Consult past industry advisories, summaries, and vendor-initiated bulletins, and follow the instructions that are relevant to your particular configuration. Verify that you have installed all applicable patches or workarounds described in the industry publications.

Caution use of data from backups

When restoring data from a backup, ensure that the backup itself is from a non-compromised 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.

Change passwords

After all security holes or configuration problems have been patched or corrected, change **ALL** passwords of **ALL** accounts on the affected system(s). Ensure that passwords for all accounts are not easy to guess.

Security Improvement

The results of the intrusion analysis will specify the method(s) employed to compromise the system. The following is a general list of improvements that may be applicable:

Passwords

- Weak passwords. Encourage your users to choose passwords that are difficult to guess.
- Accounts without passwords or default passwords. Remove extra UID 0 accounts, accounts with no password, or new entries in the password file. Do not allow any accounts without passwords. Remove entries for unused accounts from the password file.
- Reusable passwords. Use one-time passwords, especially for authenticated access from external networks and for access to sensitive resources like name servers and routers.

Prevent the use of TFTP (Trivial File Transfer Protocol) to obtain password files.

Misconfigured anonymous FTP.

Ensure that you are running the most recent version of ftpd, check your anonymous FTP configuration. Do not use your system's standard password file or group file as the password file or group file for FTP. The anonymous FTP root directory and its two subdirectories, etc and bin, should not be owned by ftp.

Use only secure protocols, ssh, scp, secure ftp.

Inappropriate file and directory protections

Check your system documentation to establish the correct file and directory protections and ownership for system files and directories. Examine file and directory protections before and after installing software or running verification utilities.

Old versions of system software

Replace older versions of operating systems known to have security vulnerabilities. Keep the version of your operating system up to date and apply security patches appropriate to your system(s) as soon as they become available.

Inappropriate export settings for UNIX systems.

Ensure that the configuration of the files on your hosts are correct.

- Wherever possible, file systems should be exported read-only.
- Do not self-reference an NFS server in its own exports file. That is, the exports file should not export an NFS server to itself nor to any netgroups that include the NFS server.
- Do not allow the exports file to contain a "localhost" entry.
- Export file systems only to hosts that require them.
- Export only to fully qualified hostnames.
- Ensure that export lists do not exceed 256 characters (after the aliases have been expanded) or that all security patches relating to this problem have been applied.

Vulnerable protocols and services

Ensure that only those services that are required from outside your domain are allowed through your router filters. In particular, if the following are not required outside your domain, then filter them out at the router or firewall.

Reconnect to the Network/Internet

Once the intrusion has been analyzed, the system has been restored, and the vulnerability that permitted the compromise removed reconnect the computer(s) or network device to the network. Monitor the system for failed attempts and/or unauthorized accesses to verify that the effectiveness of the repair.

Update your security policy or policy implementation statement

Document lessons learned from being root compromised.

Document and review your lessons learned from going through the process of recovering from a root compromise. This will help you decide the appropriate revisions necessary for your security policy.

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 give you a measurement as to the importance of security for your organization. You may find calculating the cost of this incident useful for explaining to management that security is important to your organization.

Incorporate necessary changes (if any) in your security policy.

The last step to take in this process is to make the changes to your security policy. Be sure to inform members of your organization as to the changes that have been made and how that may affect them.

5. Appendices

Appendix A - Intrusion Checklist

1. Examine log files for connections from unusual locations or other unusual activity.
2. Look for scripts everywhere on your system, especially in the /temp directory.
3. Check your system binaries to make sure that they haven't been altered.
4. Check your systems for unauthorized use of a network monitoring program, commonly called a sniffer or packet sniffer. Intruders may use a sniffer to capture user account and password information.
5. Examine all the files that are run by 'cron' and 'at.'
6. Check for unauthorized services.
7. Examine the password log files on the system and check for modifications or suspicious entries.
8. Check your system and network configuration files for unauthorized entries.
9. Look everywhere on the system for unusual or hidden files (files that start with a period and are normally not shown by 'ls' or ‘dir’), as these can be used to hide tools and information (password cracking programs, password files from other systems, etc.).
10. Examine multiple machines on the local network when searching for signs of intrusion. Most of the time, if one host has been compromised, others on the network have been, too.

Appendix B – Incident Response Worksheet

(https://www.wright.edu/cgi-bin/incidentresponse.cgi)

Appendix C – Notification Chart

*(*http://www.wright.edu/sites/www.wright.edu/files/page/attachments/Incident%20Response%20Plan_Point%20Of%20Contact%20List.pdf*)*