

# OPERATIONS MANUAL: Stage 1 - Active: Response Phase

Hal Flynn 2000-05-11

## OPERATIONS MANUAL Information Protection Center

---

### OPERATIONS MANUAL: Stage 1 - Active: Response Phase

The highest priority task for the IPC is to respond to incidents as they occur. This may involve working with the affected organisation to determine the cause of the incident and help them to become secure again, or it may involve finding a solution to a vulnerability that is actively being exploited to compromise many organisational assets. Reactive response is always done on a priority basis and involves three stages--containment, eradication and recovery-- followed by a post-incident analysis. Whatever is done must be consistent with security policies.

Keep in mind that careful protection of evidence for secondary analysis or prosecution:

- document every step taken in handling an incident and have the notes in the log signed by the author, verified by signature of 3rd party and stored securely--if the notes were within the daily incident log then make copies and secure these
- protect any logs by physically locking them away and optionally encrypting them  
make copies of affected system disks and protect these from alteration by physically securing them

A good primer on incident response is [Who ya gonna call?](#) by Carole Fennelly. The scenarios presented are a good sampling of the variety of situations that may arise.

The steps that must be followed are presented in the administration incident handling checklist. The following elaborates on these steps:

1. **Containment:** The IPC needs to limit the scope and magnitude of an incident. The first decision is what to do with critical information and/or computer resources. Next, a decision to shut down the system entirely, disconnect from network, or allow it to continue to run in its normal operational status so that any activity can be monitored. In the case of a virus infection, it needs to be quickly eradicated and a return to normal operation.
  - protect & proceed is normally applied as this best protects Organisational assets; the steps to follow are:
    - manage the IPC team resources
      - assign specific tasks to members
      - set timed goals like "if we don't discover how the break-in occurred in one hour then we shut down the network"

- disconnect from the network if there is any concern that the attacker may still be active
  - determine if a sniffer is running by following the steps in [Steps for Recovering from a Unix Root Compromise](#)
  - if possible, make a low level copy of the system disk for further analysis
  - reboot only if necessary as you will lose the operating processes (which haven't failed due to network disconnect)
  - optional automated control of filtering routers or firewalls by IDS
  - in special circumstances pursue & prosecute might be applied to track an attacker using keystroke monitoring or decoy (sacrificial) servers but this must be skillfully controlled and requires approval of the CIO
2. **Eradication:** Eradicating an incident entails executing the necessary procedures to remove the cause of the incident. For a virus infection, eradication is accomplished by using virus scanning software that will remove the virus from the information storage media. For an intruder, the best eradication is (1) closing appropriate systems vulnerability ports of entry, and (2) being able to recover information that will lead to a successful legal and personnel actions. To do this you need to look for changed system files, hidden files or new SUID files and make backups of log files prior to removal of malicious modifications or reloading the operating system.
- Lance Spitzner's primer [Hacked: Now What?](#) has some good instruction on how to deal with compromised Solaris hosts
  - viral scanners can be used to eradicate viral infections or some trojans
    - in some cases the standard viral scanning package of the managed desktop may not detect and eradicate the malicious code so alternate packages will need to be licensed and deployed
3. **Recovery:** Recovery involves restoring the system to its normal operational status. The length of the recovery process may be short, as in the case of a virus, or lengthy as in the case of an intruder that may have modified data or software files.
4. **Post Incident:** After the incident is over, there needs to be follow-up process to determine how the virus entered the enterprise or the entry point (system vulnerability) used by an intruder to gain unauthorized access. From a management point of view, a cost analysis may be requested to determine the cost of the incident. A follow-up report can be used to illustrate the "lessons learned" from the incident. The policies and procedures used by the organisation may require revision as a result of the incident. Additionally, awareness of incident activities in general and specific penalties for such types of activity need widespread publicity.
- some measure of the effectiveness and value of the IPC must be established to justify a business need and continued funding
  - post incident analysis must address:
    - do vulnerabilities still need to be closed
    - should there be adjustments made to user awareness or training
    - how did the incident start: what vulnerability was exploited or how was access gained
    - what information did IPC need, who did they contact
      - how could it have been acquired more quickly (new contacts needed)
    - how was the incident reported or detected
    - how was incident resolved
    - do existing procedures require updating

- should a decoy be added to lure attackers away from more sensitive hosts

---

[Admin](#)   [Passive](#)   [Protective](#)   [Detective](#)   [Assessive](#)   [Integrative](#)

Original development of these pages was supported by  
the Province of Manitoba

The content is maintained by [Andrew Mackie](#)

*Last modified: April 28, 2000*

[Privacy Statement](#)

Copyright 2006, SecurityFocus