

OPERATIONS MANUAL: Stage 0 - Passive

Hal Flynn 2000-05-11

OPERATIONS MANUAL Information Protection Center

Stage 0 - Passive

This particular IPC began with a relative "green field" for security. It had the creation of policies, guidelines and awareness initiative as its initial responsibilities. Most organisations will have some security group already in place handling policy and awareness programs.

Organisational and Departmental Policies: The IPC's activities in environmental scanning and VA give it a unique and integrated view of the organisation's security posture. The IPC will assist in policy formulation at both the departmental and organisation wide level.

- an HTML version of the draft of the Organisation's Security Policy document is on the IPC's intranet home page under Policies
- departments can add their own internal departmental policies to match their operational needs
- departmental policies that violate those of the overall policy must be explicitly documented, the risk assessed and the accountability for the residual risk formally accepted in writing and submitted to the Chief IT Security Officer (CITSO) by the Departmental IT Manager
- the IT Security Advisory Group is a cross-organisational body which meets to review policy and procedures and assists the CITSO in tuning policies and discussing new security strategies and policies

Awareness and Education: The center, in addition to the more technical side, will initiate awareness programs as well as system and network security training for system administrators and network managers. The following represent different mechanisms that will be used to educate and improve awareness:

- Advisories
- Conference Presentations
- Workshop Presentations

- Panel Sessions
- Courses
- Security Audits and On-site Consulting

An important mission of the IPC is education and awareness of its constituency on issues relating to security. Studies have shown that there is a direct correlation between the level of system knowledge of system administrators and the level of security in an information system. System education and training has the most impact in all area of system management. As stated earlier one of the IPC prime objectives to is support the system owners and administrator in their efforts to understand and implement security measures. The IPC will be proactive in all areas of network security education and public awareness by helping system administrators, providing advice, making presentations, writing articles and by being available with expertise and assistance. The IPC provides an infrastructure service.

The following represent different mechanisms that will be used to educate and improve awareness.

- **Advisories:** Advisories are issued to alter the constituency of a single issue about computer security. These are normally long living document and will be used for future reference. Examples include the announcement of a vulnerability and solution, a suggestion on an administrative manner, or the announcement of tool kits. An advisory announcing a vulnerability will contain enough information on the scope of the vulnerability (version and platforms affected), a description of the severity of the problem (including any exploitation), and one or more solutions. This will give the constituent enough information to decide how to apply the solution to its computing resources.
 - detail the format
 - describe means of distribution
- **Conference Presentations:** Presentations serve as a mechanism to discuss the latest research and trends in computer security. This will be the forum to relate to the constituency information that affects them directly, such as the number and severity of incidents, and general trends that have been determined.
- **Workshop Presentations:** Workshops will be offered to give users and the information security chain hands-on exposure to security tools and auditing techniques.
- **Panel Sessions:** This type of session allows people with different backgrounds to come together allowing a broader content. This is usually an interactive session with comments and questions submitted by the audience.

- Exercises: A "security exercise" is a short 10 to 15 minute activity that can increase the security of the information system by having the systems administrators respond to a given attack scenario. The exercises would be held in conjunction with security classes.
- Courses: Traditional education involves classrooms, lectures, and tutorials. This is the most effective way to educate the constituency. On-line tutorials are also powerful tools and allow users to remain at their desk to take the training.

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

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

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

Last modified: April 29, 2000

[Privacy Statement](#)

Copyright 2006, SecurityFocus