

Admin

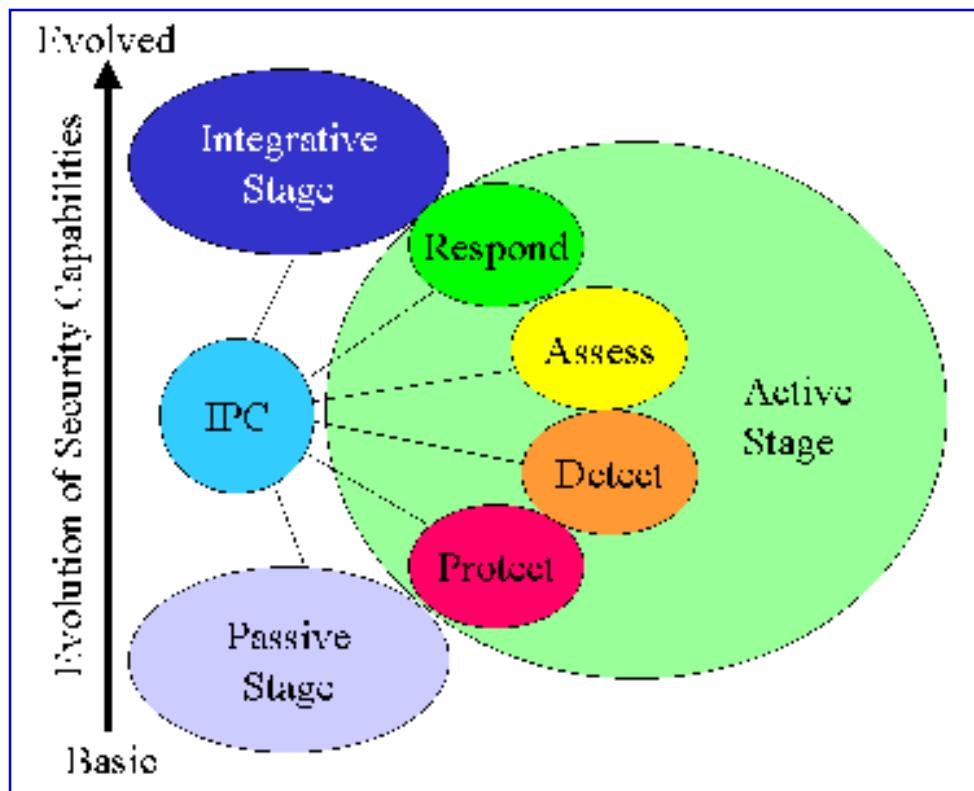
Hal Flynn 2000-05-11

Operations Manual Information Protection Centre IPC Overview

IPC Overview

Organisations rely on their networks and systems. Viral outbreaks are occurring sporadically. Their firewalls are being probed for vulnerabilities on a daily basis. It is highly likely that they will be victimized by a serious security incident at some time. The IPC provides the organised resources to address these incidents and thereby safeguard the Organisation's Information Technology (IT) assets.

The IPC evolves through three stages to reach operational maturity. Stage 0 is "Passive" security which provides a solid foundation upon which to build an IPC capability. The next stage is "Active" security which is comprised of four phases in an improvement cycle: protection, detection, assessment then response. Once these two stages have been accomplished the IPC becomes an active agent of an organisation's security program. The last phase is integrative where the IPC maximizes its collaboration with those carrying out passive security and those managers focused on business value streams. The IPC becomes involved in architectural implementation and thereby moves the organisation towards improved security infrastructure. The following represents the evolutionary stages of an IPC's capabilities (click to view larger image):



- **Passive:** a security office handling policy and awareness issues; no tools required, just travel and training budget.
- **Active Protection:** rudimentary IPC forming from security office with the addition of tools and some number of people capable of establishing Rules of Engagement (e.g., firewall policies), auditing logs, employing the tools assessing the results and assisting clients in improving their security posture.
- **Active Detection:** IPC begins to become more cognizant of environment, inserts monitoring (e.g., IDS, tripwires, viral scanning, net mapping) into infrastructure to detect malicious or unusual events. Cost to the organisation is for technology and more capable technical expertise.
- **Active Assessment:** Gather together all possible sources of incident information, correlate these and assess whether they are false alarms or verify they are significant incidents. Establish priority for incidents and carry out triage when the incidents overwhelm the resources available.
- **Active Response:** IPC capable now of acting to limit damage from significant incidents, either via automated systems or manual procedures. The IPC has become an Incident Response Team (IRT). Cost to the organisation is for availability of team members and call-in.
- **Integrative:** The knowledge and awareness of the IPC is directed towards architectural configuration control and selection of new technologies. No significant cost incurred but

this requires that the organisation has an architectural control process that includes the IPC.

The IPC provides Network and Computer Incident Response as well as co-ordination, communication and co-operation with other security agencies such as the local Police, the RCMP, CSE and CSIS. The Centre can also participate in worldwide incident response organisations such as the Computer Emergency Response Teams (CERT) and the Forum for Incident and Response Teams organisation (FIRST).

An IPC can begin as a collective of conscientious IT staff informally handling incidents in order to keep operational. Such expertise needs to be cultivated and retained through a formal mentorship program so that corporate knowledge is maintained over the longer term. This requires explicit backing from management and is best achieved by establishing permanent staffing and budget.

An IPC with limited staff will tend to have a limited depth of maturity, focusing mainly on a few capabilities. More staff and budget allows improved maturity of processes, time to improve the way things get done and deeper strengths across all capabilities. It is up to the IPC to show the value it delivers and project the return on investment of additional staffing and budget. It is up to management to keep control of staffing levels and budgets, finding best value for its money.

Administration

There are a variety of administrative tasks that the IPC must deal with:

Daily Checklist	External Contact Checklist	Equipment Inventory
Bi-weekly Checklist	News Media Handling Checklist	
Quarterly Checklist	New Software Handling Checklist	
Yearly Checklist	Malicious Code Handling Checklist	
	Incident Handling Checklist	

Daily Checklist

Raison D'être: IT Security Policy states "protecting the privacy of citizens' information while providing secure and efficient management of this information and while providing secure and efficient management of this information is critical to maintaining public confidence and delivering organisational services"

Review of newsgroups, Internet news feeds, peer networking, and paper media for new products, tools or software

Review of CERT, CIAC, Security Focus, Bugtraq etc for the latest vulnerabilities, and the subsequent distribution of information to those effected

Re-assessment of security posture based on latest vulnerability searches

- dissemination of serious issues to entire team verbally or via email

Visual inspection of integrity of physical premises and production assets to check for possible break-in or tampering

Manage secured repository of passwords for production systems and applications

Review of automated network map for unusual changes

Review firewall logs of all managed firewalls, especially any used by IPC itself

Review ID system events and do a cursory review of logs to detect network events or system problems (e.g., file space limits)

Document any changes to configuration of production tools or devices in daily log

Maintain a log of all actions and incidents worked by the team.

- a log book with permanent pages used to record ongoing activities
- each page signed by the author for the events recorded and co-signed by another individual
- old log books stored in the safe
- events or detailed investigations will be logged in a word file
- all such files will be archived in safe with a backup copy signed by the author using their private key

Maintain log of contents of safe

Maintain operational status of production tools/devices in operation

- plan for repair/recovery of failed tools/devices
- plan for insertion of new tools/devices/versions following successful test bed analysis and trial

Immediately handle situation when IPC member leaves and no longer requires privileged access

- individual leaving is to pass on any relevant files or records to manager, return all keys, passes, encryption keys, HW, SW and documentation
- manager is to ensure individual's access to IPC systems and rooms is canceled, accept all relevant records, files and IPC assets and retain all security related items (keys, badges, etc.)

Bi-weekly Checklist

Test security controls and policies of firewalls and IDS under IPC audit supervision

At bi-weekly security meetings

- The IPC needs to advertise that users are to contact either the help desk or the IPC directly when they suspect an incident has occurred
- Helpdesk and others involved in operations need to be kept informed as to IPC activities and services

Secondary analysis--ID system logs for the previous 2 week period need to be inspected closely to detect if any vulnerabilities the analyst knows are being exploited or if there are unusual patterns of activities

- this can catch events that go below the threshold of ID systems
- if a Coordination Centre exists they can assist with this activity
 - a successful model is to develop a **healthy** competitive spirit between local and secondary audit teams to see who finds the malicious events first

Inform management and the constituency about incident levels, intelligence on attacks, and a measurement of progress or success

Monitor feedback from seniors and address problems with reputation or goodwill

The IPC Director needs to manage work quality by reviewing the checklist activities and daily logs from the previous weeks

- Director of IPC maintains list of deliverables, active events and services and allocates resources and target dates towards these
 - people, time, space, money and production tools are the critical resources
 - scope of services covers the organisation itself but, if resources permit, may be extended beyond this constituency at the discretion of the CIO
- Status of any tool or product testing or trials is tracked
- Review of logs may lead to analysis and recommendations for adjustment of automated policies. Status reports may lead to re-allocation of resources, alteration of priority issues, need for more staff, etc.

The IPC Director meets with superior at least bi-weekly to discuss progress and problems or issues that need to be addressed to ensure that the IPC continues to be of value

- an ongoing risk is that the IPC will be a target since it competes for limited resources and can be seen to be an obstacle
- the risks of problems or issues need to be addressed as they could affect the viability of the IPC
- the IPC needs to be seen to deliver value, otherwise it will become a liability to the CIO
- The Director needs to maintain ties to other IT Directors to detect issues and mitigate them if the risk is high
 - ongoing vulnerability analysis (VA) will bring the IT Directors in contact with IPC and provide opportunity to reduce the tension through cooperation
 - IPC offers services and assists in delivering solutions

The IPC Director is responsible for the security and assurance of the IPC itself. Careful attention must be paid to protecting the integrity of the tool suite used by the IPC.

- wherever possible original vendor supplied CDs safely stored and used as installation medium
- network distributed software downloaded from vendor sites and original backup stored safely
- production security servers protected by firewalls which restrict incoming services
- integrity codes calculated (e.g., tripwire) for each tool and codes stored safely
 - integrity checking carried out on each tool quarterly or as required
 - integrity checking carried out using archived baseline file signatures
- wherever possible, alternate tools are used (i.e., vulnerability probing) to verify correctness of results

Maintain contact lists with duty and phone numbers, FAX numbers, E-Mail addresses and encryption keys of persons to be notified during an incident

Maintain a call-in list of personnel to act as POCs in case the team is overloaded with incidents or the nature of an incident requires a technical specialty not available from the IPC

Maintain list of those with access (combination) to safe

Quarterly Checklist

Track progress of training plan and adjust to accommodate new conferences, courses or topics

- record training taken and apply as training (e.g. CISSP recertification) credits
- IPC staff write up an assessment of effectiveness of any training they take
 - indicate any useful training materials
 - store training materials in IPC library
 - training materials are kept by IPC until they become outdated

Train team on latest intrusion detection techniques and rehearse with mock attacks or controlled penetration tests. The IPC will rely on extensive mentoring and training by peers--true information sharing within the team

- ensure team members know how to use the production tools
 - maintain documentation of production tools
 - have team members first use tools under guidance of more experienced person
 - more experienced members review the results and activities of first few uses of tools by less experienced members

Take steps to involve and mentor individuals from outside the IPC so as to maintain a pool of potential candidates should the IPC membership change

- candidates can be found in local security interest groups, Co-ops, post grads doing research, contractors

Review IT Security Policy and Guidelines which provide guidance and standards for system administration and ensure that IPC is complying

- the goals are to keep files from being corrupted or accessed by unauthorized users, to keep hardware as failure-free as possible, to keep up performance (stay operational) and to keep data safe

Review backup strategy to ensure that IPC is compliant

- backups of data from production servers are made as they are required
- production servers do not support users, only specific applications so they do not change
 - initial backups are made of the system as they go into production
 - integrity checking (e.g., tripwire) is used to establish baseline file signatures for production applications and these signatures are stored in the safe
 - records are kept of what was involved (loaded) onto the production systems
 - original distribution media is stored in the safe
- local files on the desktop or on laptops of IPC members are backed up as they feel is required

Review contents of safe to ensure nothing is missing; use maintained log of contents and correct/investigate as required

Manage change to passwords for operational systems and applications and update secured repository

Review policy and guidelines documentation and initiate dialogue with IT security representatives if update is necessary

Evaluate IPC operations against SSE-CMM criteria to measure changes against original baseline to determine where improvements are necessary

- Director must determine a reasonable distribution of resources to deliver sufficient scope of capabilities and maturity of processes to keep the IPC a viable and valuable entity within the organisation
- Director must get the commitment of the the IPC members to strive to deliver quality services
- events, altered priorities and availability of resources will affect strict adherence to the checklists so maturity will be fluid

Yearly Checklist

Prepare yearly training plan and budget for IPC members

- each IPC member must develop their IPC-related skills by attending workshops, conferences, etc.
- CISSP certification through ISC2 (www.isc2.org) would provide a structure for maintaining recertification and thereby maintaining skills
 - IPC members don't have to be certified; can simply follow the recertification criteria

Review disaster recovery planning and ensure IPC preparedness

- Critical assets are listed , the list is prioritized + identify those with responsibility for and authority to access each asset that needs to be recovered, under what conditions and by what means
 - IPC Director has full authority and responsibility
 - first priority is protective via the perimeter--maintaining or tightening perimeter controls
 - work with outsourced firewall managers to get firewalls functional
- second priority is detective--need to have indications and warnings up via IDS and network mapping
 - work with managers of perimeter controlled networks to get IDS

- engines functional
 - IPC to get IDS control systems functional
 - IPC to get net mapping functional
 - restore any decoy hosts or tripwire capabilities
- third priority is the team's assessive and responsive capabilities which derive from the availability of technically capable people
 - Director of IPC to make sure people are available
 - optional automated assessment and response linking IDS to routers or firewalls can be redeployed
- establish firecall procedures that will provide operational continuity should there be a significant risk of prolonged failure or disruption. An example would be an incident that consumes the system administration staff of an organisation, thereby not allowing the day-to-day operations (the care and feeding of operational systems) to continue. A firecall could be issued to bring systems administrators from other organisations to the affected organisations to support normal operations.
- off-site operations (hot site)
 - the IPC may well develop into a hot site for outsourced management of the network if it establishes its own network mapping and management view
 - the IPC could relocate to alternate offices

Culling of outdated training and other technical material from IPC library

External Contact Checklist

Handling difficult contacts should be gentle, courteous, considerate--they are our customers

In cases of phoned in security incidents, handle unauthenticated callers by getting someone else to verify who the caller claims to be or at least call back to the person's published phone number

- establish an IPC contact phone number with voice mail
 - keep forms with required incident information fields by phone
- establish an IPC contact email account
- assign responsibilities for daily review of messages
- feed reported incidents into tasking and incident tracking system

Disclosure of incident information must be vetted by the IPC's Director

Establish encrypted mechanisms for incident information sharing between IPC team members or with other CIRTs/IPC

Monitor feedback and pass comments as to IPC performance to Director

News Media Handling Checklist

Define set of mutually agreed upon information that can be released (e.g., severity and number of incidents, and the type of incidents being observed)

The media representative is Director of IPC, Senior Management above IPC or a specially designated media representative

- avoid revealing overt technical details
- deal only in facts--no rumours
- be aware that inflammatory statements may make your organisation a target and draw fire not only from the outside (e.g., cracker community) but also from those within the organisation that would prefer to keep a low profile in hopes that they can continue to get by with minimal security

New Software Handling Checklist

Each security tool (VA probing, IDS or FW), or version of tool, must undergo verification and validation before going into production; the same is to be applied to any tool used within the production environment (e.g., freeware download). The intent is to prevent contamination of production environment.

Environmental scanning will provide list of potential tools and "pedigree" of these tools. There are no perfect guarantees and source code will usually not be available for inspection so verification and validation that the tool does what it is supposed to do, and no more, must begin with review of available product literature, independent testing and then rely mostly on internal IPC testing. This is why the "collaborative free source" initiatives are popular in the security community.

Wherever possible, an isolated test bed is to be used for initial testing then the tool will be used on the live network for a trial period before acceptance and use as a production tool.

Initial test bed testing and trials exercise the features which would be useful for IPC activities. Network activities are monitored to detect any unusual activities. In particular the IPC is to look for packets or events that are not necessary to the operation of the tool or which would violate security policies of the production network.

Results of the literature review, testing and trials are documented to justify the use of the tool.

The concern is that a tool contains some undocumented, hidden bomb with a slow fuse or unusual trigger event. It is hoped that environmental scanning will detect indications of such malicious intentions or activities of the authors. This is why the "pedigree" or lineage of the tool is important--"freesource" code or applications that have been vetted or formally evaluated by independent third parties carry with them higher assurance

Malicious Code Handling Checklist

Assess and investigate incidents to ensure they are not false alarms

Viral incidents are usually detected either by desktop malicious code ("viral") scanners or by file server scanners and incidents are reported to Helpdesk support who assists in the cleansing

- statistics are maintained by Helpdesk support
- IPC tracks response time from first indication of malicious code to time new signatures have been distributed
- IPC attempts to minimize the time taken to update viral signature databases on servers, desktops and email gateways

In cases where malicious code is not detected by automated scanners, they may be detected by unusual activity reported to the Helpdesk. Support personnel will determine source of problems and resolve them

- IPC may need to use viral scanners from alternate vendors to provide wider coverage and eradication services

Get accurate information out to all users

- work with Helpdesk Security Point of Contact (POC) to do this
- track authorities on Internet for indication of current analysis
- once analysis provides significant results that would assist users, get this info out as well

New viral signatures need to be distributed to all desktops, servers and scanning gateways

- user notification should include all users environments
- message should include link to source of new viral signature file or product non-managed users can employ

See OPS Manual covering "Assessive and Responsive" capabilities for further advice on handling incidents in general

Incident Handling Checklist

Incident reporting is done through the Incident Report form provided on intranet IPC web pages



-  click on thumbnail for large image of form

Assess and investigate incidents to ensure they are not false alarms

- most ID systems err on the side of caution and signal alarms for anything suspicious so don't overreact
 - carefully analyze the event and try to understand what the ID system is telling you and whether it is a serious incident
 - if you are using a network ID system that relies on passive sniffing then it may not attempt to distinguish between "outside" and "inside" because addresses could be spoofed; this means you can be seeing events from suspect activity in both directions so you need to resolve this to establish how to respond to the incident (i.e., are you under "attack" or is it someone from within your organisation "attacking" an external site)
- compare the activity to see if it is "normal" business by checking with the System Administrator or system owner(s) involved
- resolve the addresses using services such as www.arin.net/whois
- compare the activity against previous activities in the logs to see if the same source has been involved in other activities
- assess whether the activity could have compromised your systems or was contained by the existing security controls in place

If you feel the suspect activity may have succeeded in bypassing your controls and compromised one or more systems, you can no longer trust your network so don't disseminate information regarding the incident via cleartext email. Use encrypted messages or phone.

The next step in assessing a security incident is to consolidate what you have found out and record this

- Is the incident a penetration attempt or a violation of the security policy?
- Is the incident presently active?
- What is the source of the incident?
- Has the system been compromised?
- Which organizations are involved?

Notify the Director with this information. She/He will have to notify senior managers

Responses in case of violation of security policy

- Because security policy violations are committed by internal users, some delicacy is required to handle the situation since it may result in legal action. It is very important to involve senior management first then, if necessary, Legal, and Human Resources to limit the company's exposure to liability
- The IPC will inform senior management and follow Human Resources guidelines
- If the CIO so directs, the IPC will discreetly gather all necessary information and save to backup media
- a complete report will be provided to CIO who then deals with it as a management issue

Responses in case of technical attack assign CyCon level of organisation (see OPS Manual on responsive capability)

1. noise level, no detected attacks
2. unauthorized scans, sporadic attacks detected
3. coordinated hacking attempts or DoS detected
4. successful attack(s) detected, containment, eradication and recovery necessary
5. under heavy assault, facility shutdown and firecall procedures required (see yearly Checklist)

In case of attacks at CyCon 4 or 5, the CIO is to decide whether the IPC is to follow up by contacting the originating ISP's technical contact. In any case the IPC must be more vigilant in its monitoring of log files.

Track the status of each incident until it is resolved using the IPC's internal incident database

- report final status to those who submitted incident report (details may be vetted)
- status reported to Helpdesk if they were involved and established trouble ticket
- generalized report without sensitive details can be posted on internal security web server

Details of the incidents at CyCon level 4 or 5 should be discussed only on a need-to-know basis, as approved by senior management

A chronological log must be maintained of all investigative measures. This log might be used as legal evidence so it is to be signed by all involved members of the IPC

A backup should be made of the data, preferably on write-once media. At the very least, the media should be write-protected

See OPS Manual covering "Assessive and Responsive" capabilities for further advice on handling incidents

Equipment Inventory

The list of equipment typically used by the IPC:

- PC desktops for each member of the IPC
- Laptops for each IPC member
- IDS console in production
- Window grabber SW to capture images of incident related info
- IDS monitoring engines throughout environment
- Network vulnerability scanners
- Linux platform running freeware security tools

Optional:

- Host-based IDS
- Network discovery tool
- Secure extranet service

Software used to develop documentation:

- MS PowerPoint
- MS FrontPage
- MS Image Composer
- Corel Web Designer

Passive 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 28, 2000

[Privacy Statement](#)

Copyright 2006, SecurityFocus