Incident Response Plans
What to do when things go south
Incident Response Plans

- The complex nature of cyber incidents demand incident response plans that are concise, flexible, and cover commonly encountered situations.
- These include DoS attacks, PCI/PII theft, intrusion, insider attacks, and virus incidents.
Preparing and planning

- Think of an Incident Response Plan as a mini-business continuity plan (BCP).
- As with a BCP, first perform a risk assessment and identify resources you want to protect.
- A risk assessment is a business process, so include decision makers from affected areas.
Preparing and planning (cont’)

- Analyze resources to protect
- Rank according to C - I - A
- Assign a dollar value
- Determine minimum threshold for each resource to declare an incident
- Determine resources needed for response
- Do your homework and see what resources are required by regulation or contract
Notification

- Local bosses and staff as needed
- Law enforcement (determine who can contact law enforcement up front)
- Incident response teams
- Affected and involved sites
- Internal communications as appropriate
- Public relations and press releases
- Legal counsel
- Service Providers (DoS, Web site breaches)
Notification (cont’)

- Identify in-band and out-of-band communication channels
- Phone numbers, phone numbers, phone numbers
Identifying an incident

- Is a port scan an incident?
- Does it require a response?
- Determine threshold for declaring an incident for each protected resource
- Denial of Service attack
- PII/PCI resource breaches
- Virus/Worm
- System Compromise (insider/external)
Handling

- Large organizations may have full-time incident handlers
- For most SMEs this is an supplemental duty
- Recognize that some incidents may take longer than anticipated (days, weeks)
- Identify people who can take up the slack for the part-time incident handler
Handling (cont’)

- Notification (who should be notified)
- Protecting evidence and activity logs (what records should be kept from before, during, and after the incident -- do your homework there may be regulatory requirements)
- Containment (limit the damage)
- Eradication (eliminate reason for incident)
- Recovery (going back on line)
- Follow Up (lessons learned)
Aftermath

- Reorganize and prepare for counter-attack
- Lessons Learned - what weaknesses are exposed by the incident?
- Develop plan to address the weaknesses.
Administrative Response

- Were resources adequate?
- Changes in plans/rosters etc.
- Support from leadership
- Identify coordination snafus
Incident response plans need to be living documents taking into account the situation and available resources. Because of their complexity, incident response plans should be periodically rehearsed, deficiencies noted, and revised. Rehearsals will also reveal areas where additional training is required for the incident responders.
Incident Handling Plan Resources

- RFC 2196 Site Security Handbook Ch. 5 - http://www.faqs.org/rfcs/rfc2196.html
- AICPA/CAIA* – Incident Handling Template - http://infotech.aicpa.org/resources/privacy/

* American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants
Virus Incident Response Resources

- Sandboxes
  Anubis - [http://anubis.iselab.org/](http://anubis.iselab.org/)
  Norman Sandbox Information Center
    [http://norman.com/microsites/nsic](http://norman.com/microsites/nsic)
Some vendor virus sample drop sites
- http://www.webimmune.com
- http://sophos.com/support/samples/
- http://www.f-secure.com/virus_sample

Virus detection comparison drop site
- http://www.virustotal.com/
Virus Incident Response Resources (cont’)

- Analysis & cleaning (not vendor centric)
  - HijackThis!

- Various Rootkit Detectors
- AV standalone cleaners