# Incident Response Training and Workshop Oct 28, 2010

Ralph Durkee
Durkee Consulting, Inc.
rd@rd1.net

# Ralph Durkee

- **Founder of Durkee Consulting** since 1996
- President, Rochester ISSA Chapter 2010, VP 2004-09
- **Rochester OWASP Founder** since 2004
- **SANS Certified Incident Handler** since 2001
- Teaching SANS courses since 2002
- **Application Security**, development, auditing, PCI compliance, pen testing and consulting
- **CIS (Center for Internet Security)** – Development of benchmark standards – Apache, Linux, BIND DNS, OpenLDAP, FreeRadius, Unix, FreeBSD

# Agenda

- Introduction
- Incident Response Process
- Incident Response Team
- Roles & Responsibilities
- Communication
- Records & Evidence
- Common Issues

# Why an Incident Response Training and Workshop?

- To be better prepared to respond to and limit consequences of incidents
- To stay familiar and up-to-date with the CIRT process
- To test and identify ways to improve CIRT process and related processes
- To meet CIP 008-3 requirements for testing CIRT

CIP 008-3 R1.6 Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

# Definitions

- Incident Response
  - Process for identifying and responding to computer security incidents
- CIRT – Critical Incident Response Team
  - Coordinated team composed of multiple teams prepared to identify and respond to incidents, including**: Incident Management Team (IMT)** and **Incident Action Team (IAT)** and **Business Management**
- Security Event
  - A recorded or observed occurrence of interest on system or network
- Incident
  - A violation of company information security policies
  - An event that poses a risk to your organization's information resources or assets

# Incident Response Standards

- National Institute of Standards and Technology (NIST)
  - “Computer Security Incident Handling Guide” SP 800-61 Rev. 1 Mar 2008
    - Organizing a Computer Security Incident Response Capability
    - Handling an Incident
- SANS / Department of Energy Incident Response Process
  - Taught via SANS Sec504
  - GIAC GCIH Incident Handlers Certification

# INCIDENT RESPONSE PROCESS

# Incident Response Process

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Post-Mortem
7. Reporting

# NIST Incident Response Process

**Defined sp800-61 - http://csrc.nist.gov/**

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, Recovery
4. Post Incident Activity

# Incident Management Preparation

- **Preparation** is an important explicit step in the process
  - Preparation is critical to the success
  - Needs to have appropriate time and resources
  - Needs to be continuous and up-to-date
  - Implements lessons-learned from previous incidents
  - Lessons-learned can also come from
    - False positives
    - Workshops and incident response drills
    - Incidents in the news (learn from others mistakes

# 1. Preparation

- Preparation essential to the effectiveness of the Incident Response Process
- Ensure policy, processes, information, people, tools, skills and other resources are available and up-to-date.
- Monthly or Quarterly meetings recommended to review current state and next steps

# 2. Identification

- Starts with an event of interest
- Assign Incident Handler to investigate
  - Requires IR technical skills to investigate
  - Needs understanding of IR issues
  - Keeps in communication with IR management team
- Declares Incident or Not
- Reports finding to IR management team
- IR Management Team included as needed according to areas of responsibilities

# 3. Containment, Eradication, Recovery

1. Short term containment – Limits the damage while avoiding modifications
2. Forensic Backup w/ chain of custody
3. Long term containment – Modifications to prevent additional damage
4. Eradication – Getting rid of the

# 4. Post Analysis / Lessons Learned

1. Lead handler or Incident Manager writes up first draft of Incident report and circulates to IR Team
2. Discuss, modify and reach consensus on Incident report with IR team.
3. Document lessons learned and action items for preparation phase

# Management Reporting

- Executive Summary from past incidents
- Highlight processes and controls that worked
- Estimate savings due to IR process
- Include status on IR preparation efforts
- May include news on related incidents to other similar business
- Possible Kudos to those who reported events

# INCIDENT RESPONSE TEAM

# Incident Response Team (IRT)

- **AVAILABLE** - An incident response team should be available for contact by anyone who discovers or suspects that an incident involving the organization has occurred.
- **SIZE** –
  - During Analysis - One or 2 team members,
  - Rest of the time - 2 or more depending on the magnitude
- **TEAM** - The incident handlers work together to analyze the incident data, determine the impact of the incident, and act appropriately to limit the damage to the organization and restore normal services.
- **EXTENDED COOPERATION** - Although the incident response team may have only a few members, the team's success depends on the participation and cooperation of individuals throughout the organization

*National Institute of Standards & Technology

# IRT Centralized Model

- Central Incident Response Team
  - A single incident response team handles incidents throughout the organization.
  - This model is effective for small organizations.
  - The centralized incident response entity facilitates incident management, standard practices and communications among the team members.

# IRT Distributed Model

- Distribute Incident Response Team
  - A incident response team for each major location throughout the organization.
  - Centralized reporting and management
  - This model is effective for larger organizations.
  - The central incident response team facilitates standard practices and

# IRT Team Staffing

- Incident response teams can also use any of three staffing models:
  - Employees
    - The organization performs all of its incident response work, with limited technical and administrative support from contractors.
  - Partially Outsourced
  - Fully Outsourced
    - Still Requires IRT for oversight and business decisions

# IRT Considerations

- **The Need for 24/7 Availability.**
  - Incident handlers and team members can be contacted at any time by phone or pager, may also mean that an onsite presence is required
- **Part-Time Team Members**
  - Procedure is most critical to smaller organizations since IRT members are not full time incident handlers.
- **Employee Expertise and Morale**
  - Team members require continual training to update experience on IR skills and knowledge.
- **Cost**
  - Cost is a major factor, especially if employees are required to be onsite 24/7. Include incident response-specific costs in budgets. Training, knowledge updates, tool skills, funds to support staff during incidents.

# ROLES AND RESPONSIBILITIES

# IRT Manager

- A team manager or duly appointed designate should be in charge of an incident.
- This responsibility is generally achieved by having an ISO as team manager and a deputy team manager who assumes authority in the absence of the ISO.
- The managers typically perform a variety of tasks, including acting as a liaison with upper management and other teams and organizations, defusing crisis situations, and ensuring that the team has the necessary personnel, resources, and skills.
- Managers should also be technically adept and have excellent communication skills, particularly an ability to communicate to a range of audiences.
- Finally, team managers should be able to maintain positive working relationships with other groups, even under times of high pressure.

# IRT Technical Lead

- A person with strong technical skills and incident response experience who assumes oversight of and final responsibility for the quality of the technical work that the entire incident response team undertakes.
- The position of technical lead should not be confused with the position of Incident Lead.

# IRT Incident Lead

- The incident lead may be
  - coordinating the handlers' activities,
  - gathering information from the handlers, providing updates to and from other groups,
  - ensuring that the team's needs are met,
  - arranging for food and lodging during extended incidents.
- Team manager, project manager or logistics coordinator
- Not generally required for small Incidents

# IRT Member Technical Skills

- Critical technical skills include:
  - system administration,
  - network administration,
  - programming,
  - technical support,
  - intrusion detection.
- Good problem solving skills;
- Real-world troubleshooting experience.
- Not necessary for every team member to be an expert
- Should having at least one highly proficient person in each major area of technology (e.g., particular operating systems, Web servers, and e-mail servers) is a necessity.

# IRT Member Other Skills

Other required skills in addition to technical expertise.

- **Teamwork skills** - fundamental importance because cooperation and coordination are necessary
- **Good communication skills** - will interact with a wide variety of people, including incident victims, managers, system administrators, human resources, public affairs, and law enforcement.
- **Writing skills** - preparing advisories and procedures.
- **Building Relationships** – Ability to get cooperation from others
- **Team Blend** - Team should have a good blend of skills, not everyone needs to be skilled in all of these areas.

# IRT Members and Other Groups

- Preparation and Participation with departments or groups is vital
- Conduct Periodic Training with these groups.
- Must rely on the expertise,  judgment, and abilities of:
  - Management
  - Compliance & Audit
  - Risk Management
  - IT
  - IT Support
  - Legal Department
  - Public Affairs and Media Relations
  - Human Resources
  - Business Continuity Planning & Support Services
  - Physical Security and Facilities Management

# IRT & Management

- Management invariably plays a critical role
  - establishes incident response policy,
  - budget, and staffing.
  - ultimately, held responsible for coordinating incident response among stakeholders
  - minimizing damage,
  - reporting to corporate officers, regulators and other parties.
- Without management, IRT can not be successful.

# IRT & IT

- IT technical experts needed
  - system administrators,
  - network administrators,
  - software developers
- Much depends on differentiating abnormal from normal behaviors.
- Requires staff which are familiar with the daily operation of the specific systems and networks
- This understanding can facilitate IRT's decisions such as whether to disconnect an attacked system from the network.

# IRT & IT Support

- IT support (e.g., help desk, field technicians)
  - have the needed technical skills to discover a potential problem,
  - Typically receive a phone call from end users admitting to honest mistakes or reporting a problem.
- These discoveries or reports can facilitate early warning and discovery.
- Reported suspected problems or concern to ISO.

# IRT & Legal Department

- Legal experts should review incident response policies and procedures to ensure their compliance with law and Federal guidance, including the right to privacy.
- Guidance of the general counsel or legal department required if there is any reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit.

# IRT & PR/Media Relations

- Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public (within the constraints imposed by company security and law enforcement interests).

# IRT & HR

- When an employee is the apparent target of an incident or is suspected of causing an incident, the human resources department needs to be involved—for example, in assisting with disciplinary proceedings or employee counseling.

# IRT & Business Continuity/Support

- Computer security incidents
  - undermine the business resilience of an organization
  - act as a barometer of its level of vulnerabilities and the inherent risks.
- BCP professionals should be made aware of incidents
  - pasts impacts can be used fine-tune business impact assessments,
  - have valuable expertise in minimizing operational disruption
  - may be valuable in planning responses to certain types of incidents, such as a denial of service (DoS) attacks.
- Ensure that IR policies and procedures and business continuity processes are in sync.

# IRT & Facilities Management

- Computer security incidents may include
  - breaches of physical security
  - involve coordinated logical and physical attacks.
- Threats made against the organization may not indicate whether logical or physical resources are being targeted.
- Often need access to facilities during incident
- Close coordination between physical security and facilities management and the incident response team is important.

# IRT & Law Enforcement

- While not required, it is good practice to establish a relationship with law enforcement officials.
- Obtain management agreement on establishing contact
- Know the scope and conditions in which they are to be requested.
- Understand their potential abilities as well as constraints before an incident.
- Sit down and discuss scenarios and share with IRT during next planning meeting.
- At time of incident, it is good to know who to call and potential actions; delays or missteps could be costly.

# Roles & Responsibilities Summary

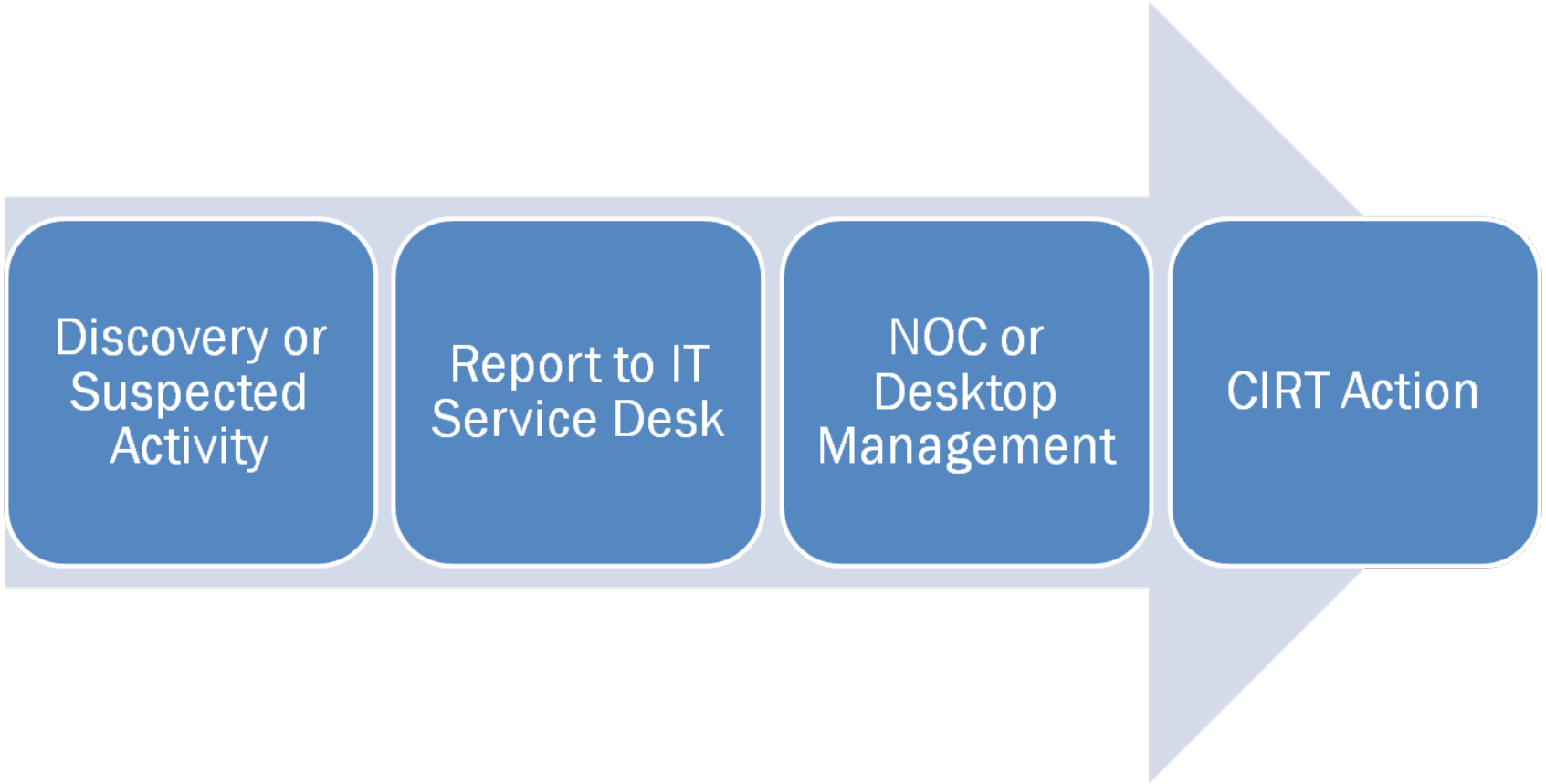
- IRT
  - Centralized function
  - One Point of Contact
  - Coordinates all Response Investigation and Activity
  - Coordinates with all internal and external organizations
  - Organizes year round training and education

# COMMUNICATION

# Reporting an Event or Activity or Concern

- Any employee may report an event or activity or concern to the IT Service Desk.
- The ISO can identify or declare an Incident.
- The ISO in conjunction with the Incident Response Team (IRT) will use standard internal procedures to log and track incidents and, working with others as appropriate, take steps to investigate, escalate, remediate, refer to others or otherwise address as outlined in the remainder of this policy.

# Incident Response Procedure



# Communication Methods by Incident Priority

- High Priority Immediate Response Methods
  - ISO
    - Face to Face on Demand
    - Cell Phone
    - Pager
- Medium Priority
  - ISO
    - Face to Face
    - Text
    - Direct Voice Line
- Low Priority Best Effort Methods
  - ISO
    - Scheduled Meeting, Best Effort Voice, Email, Voice mail

# Communication and Procedures are Critical

- Reach Desired Outcome and Protect the Organization
- Avoid Independent Action Which Can Result In:
  - Lower Quality of Work
  - Best guesses resulting in mishandled incidents, unauthorized or unbudgeted actions or not suitable to corporate direction
  - Accidental release of sensitive information
  - Higher administrative costs
  - Undesired results

# Preparation - Internal Communications

- After hours contact information
- Alternate communications
  - Cell phones
  - Fax
  - Home
- Secure communications
- Kept up-to-date
- Who’s the technical contact for an asset?

# Preparation - External Communications

- Keep contact information available, up-to-date
  - Law Enforcement Agencies
  - Internet Service Providers
  - Hardware and Software Vendors
  - Suppliers
  - Business Partners
- Public Relations
  - Define Roles & Responsibilities
  - Policy and Awareness for external communications

# Preparation - External Communications

- Requirements for Contacting Law Enforcement
  - Financial and SEC regulations
  - Privacy notification laws
  - Potential for harm to an individual or organization
  - Potential contractual obligations
- Requirement for Contacting Regulatory
  - Critical Infrastructure Protection - CIP-008-3

# Preparation – Law Enforcement

- How to decide when LEA not required?
- Benefits
  - Perception – people vs. defendant
  - Additional resources & skills
- Negatives
  - Business no longer controls the investigation
  - 2 separate cases,
  - 2 Separate motives and agenda
    - Protect the Business
    - Catch the bad guys

# Preparation – IT Vendors and Contracts

- Incident Response process and responsibilities need to be comprehended appropriately in IT contracts
- Outsourced service contracts
  - Security requirements
  - Legal and regulatory requirements
  - Audit processes and requirements
  - Processes for Incident Management

# RECORDS & EVIDENCE

# Records and Evidence

- Important to take notes from the start
- Record:
  - Verbal reports and interviews
  - Logs and observations
  - Specific actions taken
- Incident forms
  - SANS Sample forms http://www.sans.org/score/incidentforms/

# Evidence Collection and Chain of Custody

- Evidence has to be collected appropriately
- Integrity of Evidence needs to be preserved through a chain-of-custody document
- Locked in storage with restricted access
- Document:
  - What- Specific identifying information
  - Who - Name, title, phone of each person
  - When –Date and time of handling
  - Where – Location the evidence was stored o

# Evidence
# Disk Imaging

- Forensic imaging of a disk is **sector by sector**, bit for bit verifiable copy
- Can use commercial or open source tools
- Process needs to be
  - Documented, standard process
  - Tested on various platforms
  - Verified – Use secure hash and also restore & re-image
  - Performing by someone who has practiced the process.

# Disk Imaging Tools (Software)

- Open Source Tools
  - **dd** – Unix & Linux command line tool
  - **dcfldd** – Unix command line, adds secure has, progress, logs and other features
  - **winddd** – windows port of dd.
- Commercial Tools
  - **Encase**
  - **Forensic Toolkit** by Access Data

# Disk Imaging Tools (Hardware)

- Hardware Tools
  - Write Blockers, Cable and connectors with write
  - Disk Duplicators
  - Specialized forensic drive hardware duplication kits.
- Considerations
  - Need hardware to support every platform (IDE, EIDE, ATA, SATA, SCSI etc)
  - How to handle Mobile phones?

# Computer Evidence Collecting Volatile Information

- Volatile information also needs to be collected with a process that is documented, tested and verified.
- Process needs to make minimal changes to the system
- Establish a remote connection or remote login is acceptable when a necessary part of the process
- Commercial tools and Open Source tools

# COMMON ISSUES

# Issue Identification & Evidence

**ISSUE**:

- We often don't know if we need to preserve evidence until we have completed the identification.
- If it's just an event then we want to stand-down without too much effort.
- How do we get evidence to analyze the event?

**ANSWER**:

- Analyze central logs from firewalls, servers and other services
- Remote connections and Login are ok, as long as recorded.
- Avoid making changes
- Remote volatile evidence collection tools can also be used for identification
- Many possibilities depending on the event.

# Inaccurate Information

- Resist pressure to take immediate action
- Take the time to verify the accuracy of all information
- Ask Questions:
  - Who provided the information?
  - How confident are they in its accuracy?
  - Where else would this information be available?
  - Check additional sources, systems or people to verify the accuracy and to get collaboration.
- Unfortunately mistakes based on inaccurate information are way too common during incidents.

# Analyzing the Evidence

- We've collected and verified the information
- We stick to the facts in terms of taking notes
- Now we put it all together and what does it all mean?
- We have the evidence, For example:
  - Ping sweeps of several networks from a single source
  - Port scans from the same source IP address
  - Router queries about networks and routes available
  - All from a remote partner network
- What is it? Is it malicious?
- Next Steps?

# Making Assumptions

- Previous example: Sure it looks like really malicious traffic!
- What are the underlying assumptions?
- Is there another possible explanation for the evidence?
- A network discovery tool or asset management tool would have similar characteristics.
- It may not be authorized traffic, but that doesn’t mean that it is necessarily a malicious worm

# Training and Experience

- The high pressure makes incident response especially challenging
- Add the complexity of the systems, protocols, business processes, and people involved
- No one person has experience in every area of the business and area of the technology
- Need a team which
  - Remains calm, Communicates well
  - Builds on past experience
  - Works thoroughly and doesn’t panic

# Thank you!

## QUESTIONS?