Security Incident Handling

TOC

Definitions

- Incident Response
  - Any action by an organization to a defined event
    - There are many types of incidents
    - Our focus will be on technology incidents
- Incident Response Planning
  - Efforts by an organization to handle any incident
- Forensic Readiness
  - Preparedness to gather, store, and handle incident response data

What does your threat model look like?

- Internal
  - Surveys indicate ~70% percent of security threats come from the inside
- External
  - Do you have a highly visible Internet presence.
  - Are you a target of choice or a target of chance
    - Financial institutions verses panagiotiskikiras.com
- Failures
  - Does your organization require “highly available” systems
    - How much down time is acceptable

Threat Model: Internal

- Willful Destruction
- Theft
- Abuse or privilege or resources
- Accidental
  - These all have many categories but can be lumped into a few containers such as:
    - Property
    - Data
    - Resources

Willful Destruction

- Definition
  - The act of destroying; a tearing down; a bringing to naught; subversion; demolition; ruin; slaying; devastation.
- Example
  - A disgruntled employee physically destroys their laptop or formats the hard drive destroying data critical to project success

Theft

- Definition
  - The act of stealing; specifically, the felonious taking and removing of personal property, with an intent to deprive the rightful owner of the same; larceny.

    Note: To constitute theft there must be a taking without the owner's consent, and it must be unlawful or felonious; every part of the property stolen must be removed, however slightly, from its former position; and it must be, at least momentarily, in the complete possession of the thief.

- Example
  - An employee removes internal client information for sale to a competitor

Abuse of Privilege

- Definition

  To use one's legitimate access rights to perpetrate a malicious activity.

- Example:

  Comp monitors financial firm's buy and sell activity by pulling Sybase traffic from a protocol analyzer deployed to capture said data for performance analysis.

Accidental

- Definition

- Examples
  - An employee selects files for deletion on the corporate file server. But unwittingly deletes files not owned by them.
  - The cleaning crew unplugs a server so that they can plug in their vacuum cleaner.
  - The hot water heater explodes and floods the server room.

Threat Model: External

- Social Engineering
- Worms and Virii
- DDoS
- “Hackers”
- Mis-configured and unconfigured devices

Social Engineering

- Definition

  Term used among crackers and samurai for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.

- Example

  “Hello, this is Jim from Systems, we need your password”

Virii and Worms

- Definition
  - Worm - A program that propagates itself over a network, reproducing itself as it goes.
  - Virii - Unlike a worm, a virus cannot infect other computers without assistance. It is propagated by vectors such as humans trading programs with their friends. The virus may do nothing but propagate itself and then allow the program to run normally. Usually, however, after propagating silently for a while, it starts doing things like writing cute messages on the terminal or playing strange tricks with the display (some viruses include nice display hacks). Many nasty viruses, written by particularly perversely minded crackers, do irreversible damage, like nuking all the user's files.
- Examples

  CodeRed

  Stoned

DDoS

- Definition

  Distributed Denial Of Service – A resource attack to a single target originating from multiple sources
- Example
  - Yahoo, Buy.com, eBay, CNN, E*Trade, and Amazon attacks
- Tools
  - Trinoo
  - Stacheldraht

“Hackers”

- Definition

  There are many definitions, but for this discussion we’ll label hackers as “Bad Guys” attacking your systems or resources with malicious intent

- Example

  A malicious intruder exploits a vulnerability in your organizations web application(s) and retrieves sensitive customer data

Mis-configured or unconfigured devices

- Definition

  Any device placed into services before having undergone proper configuration.

- Examples
  - Default OE installations
  - Default web server installation
  - Development systems
  - “Temporary” changes for testing or other purposes
  - Devices deployed by uninformed administrators

Threat Model: Failures

Overview

- Hardware Failures
  - HA component failures not noticed
  - Gradual component failures not noticed
- Mis-configuration
  - Wireless AP breach of security perimeter
  - Unconfigured, Unused and Unknown services
  - Cascading ACLs mis-applied or mis-understood
  - Overly permissive ACLs by policy
- Software Failures

3. What is Incident Handling?

- What is a computer security **incident**?
  - **Adverse event** in information system infrastructure
  - Threat of the occurrence of adverse event
- What is an **event**?
  - **Any observable occurrence** in a system or network
  - Sometimes indicates an incident is occurring

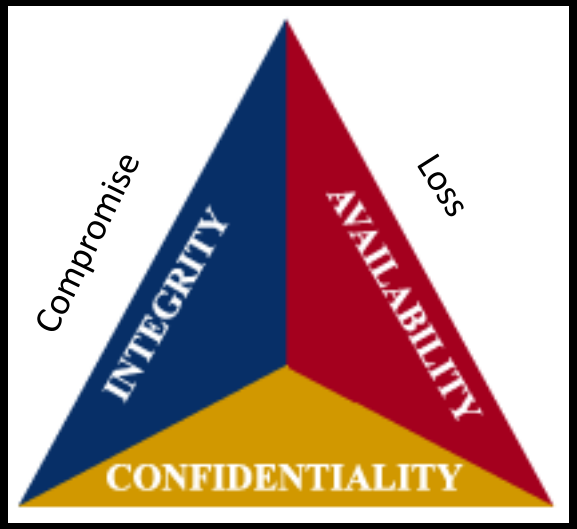
3. What is Incident Handling?

- **Incident Types**
  - Malicious code attacks
  - Unauthorized access
    - Attempted intrusion
    - Reconnaissance activity
  - System compromise/ intrusion
  - Loss of, theft of or missing assets, data, etc.

- **Incident Types**
  - Disruption of service
  - Unauthorized use / Misuse
    - Infraction of policy
    - Illegal activity
  - Espionage
  - Hoaxes (False information)

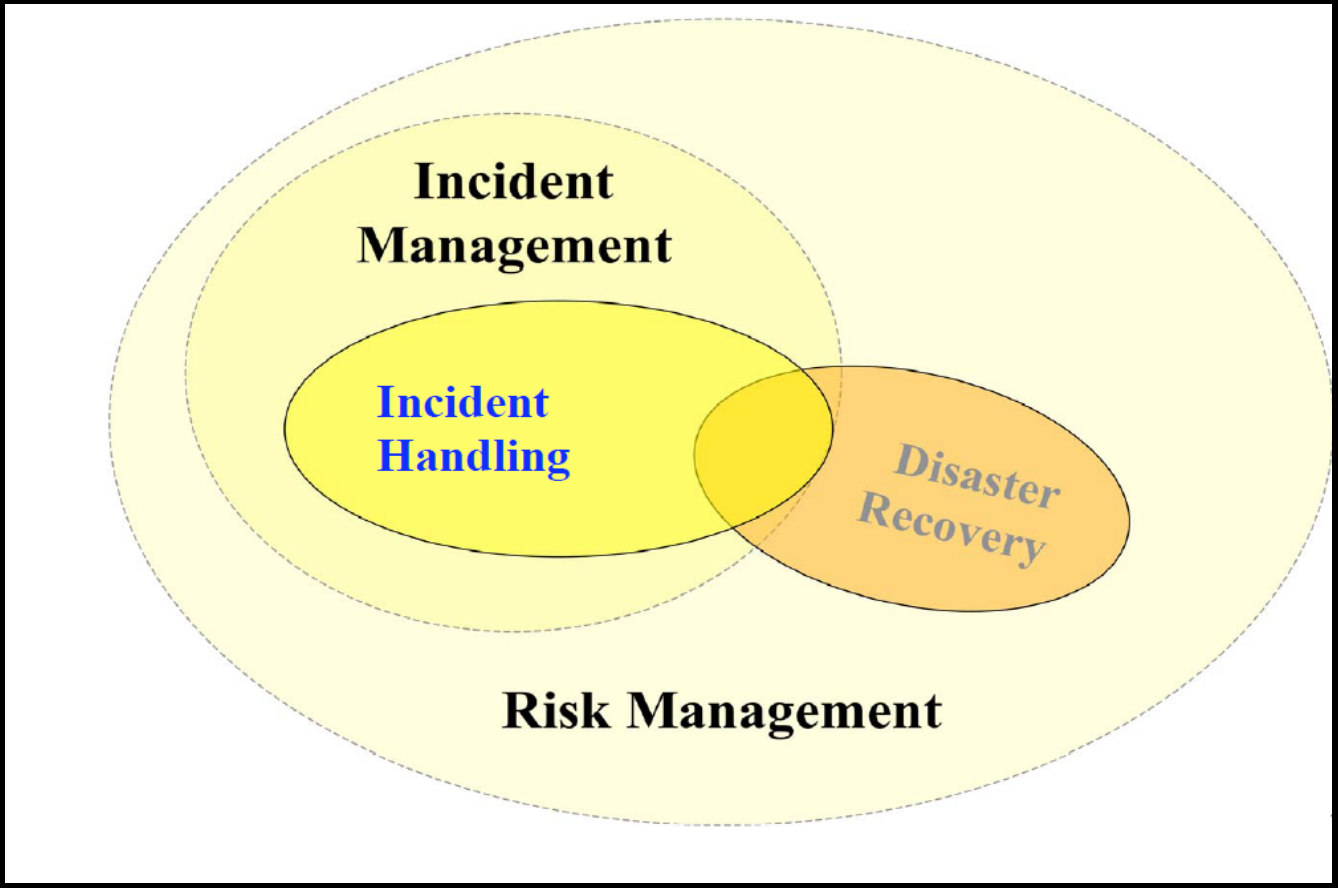
3. What is Incident Handling?

Incidents are resulting in



... of data / service / identity

3. What is Incident Handling?



4. What is Incident Management?

- **Aims of Incident Management:**
  - Restore normal service as quickly as possible
  - Minimize adverse impact on business
  - Ensure no incident goes undetected
  - Ensure incidents are handled with consistent processes
  - Reduce number of incidents in time
  - Build working relationships across organization with open communication

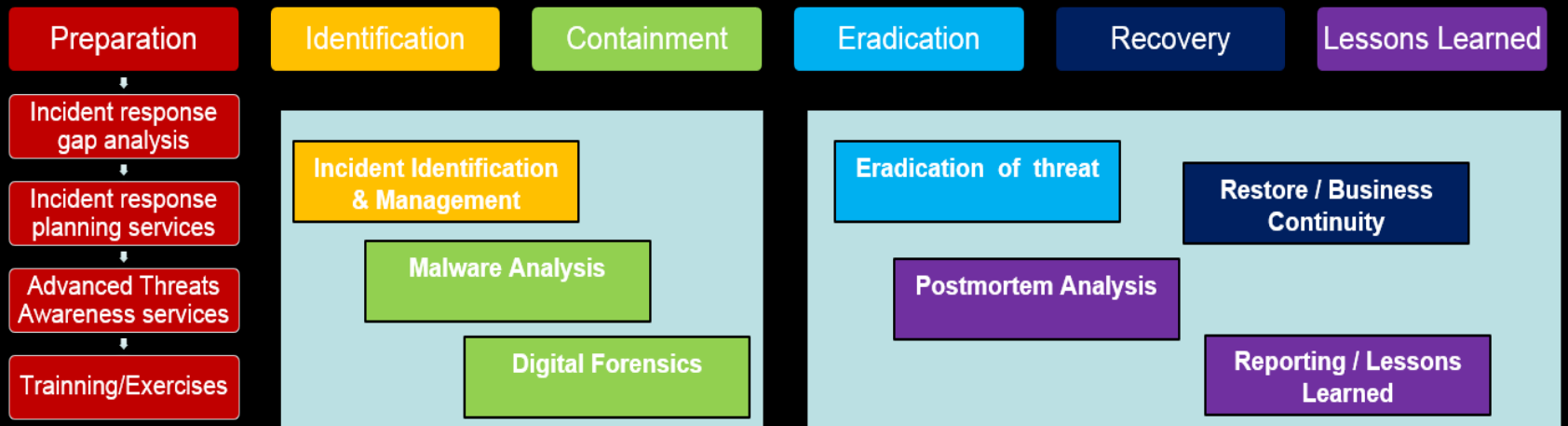
4. Why do we need Incident Management?

- Not all incidents can be prevented and anticipated.
  - ...despite risk mitigations
- New kinds of security incidents emerge with new technologies.
- Incident handling is a complex undertaking.
- Upon occurrence of incident:
  - Time to execute plans, not start thinking about them!

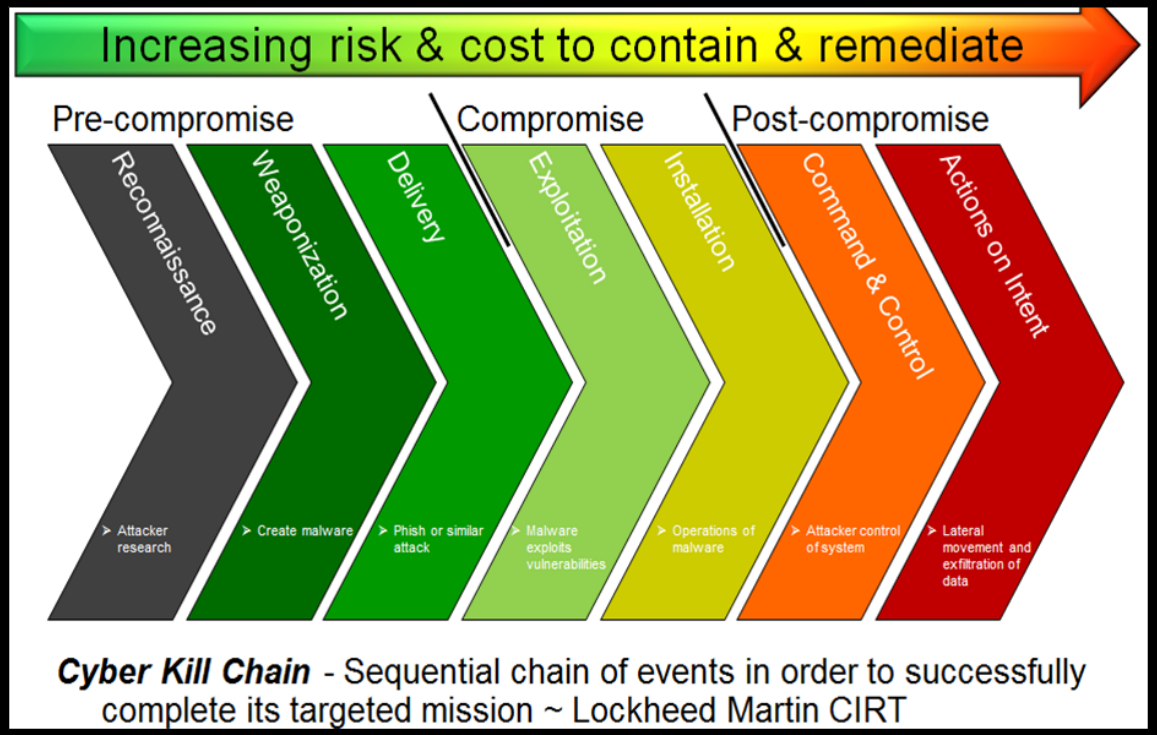
5. Six Phase Approach

- **Incident Management Strategy**
  - **1. Preparation**
  - **2. Identification**
  - **3. Containment**
  - **4. Eradication**
  - **5. Recovery**
  - **6. Lessons learned**

5. Six Phase Approach



5. Six Phase Approach – Cyber Kill chain



Cyber Kill Chain - Sequential chain of events in order to successfully complete its targeted mission ~ Lockheed Martin CIRT

5. Six Phase Approach

- **Incident Handling Strategy**
  - 1. Preparation
    - Have a game plan. Be ready
  - 2. Identification
    - Who does what and how? Where is XYZ?
    - Assessment of situation.
  - 3. Containment:
    - Close the fire gate
  - 4. Eradication:
    - Remove the threat and **vulnerability**
  - 5. Recovery:
    - Restore health. Rebuild if necessary
  - 6. Lessons learned:
    - Review what has (and has not) been
    - done. How can we improve?

5. Six Phase Approach

- **The 7 steps of preparation**
  - 1. Be proactive.
  - 2. Management support & directive
  - 3. Selection of incident response team (IRT)
  - 4. Communications plan
  - 5. Reporting facilities
  - 6. Train IRT
  - 7. Guidelines for inter-departmental or peer cooperation

The 7 steps of preparation

- Be Proactive
  - Patch management.
  - Establish, communicate, and enforce policy.
  - Establish, communicate, and enforce procedures.
  - Review policy and procedures.
  - Improve technical security skills.

The 7 steps of preparation

- Management Support & Directive
  - Have senior management's buy-in.
  - Create a formal, written security IR plan.
    - Align IR plan with business needs.
    - Include a graphical illustration of IR process. (i.e. flow chart)
    - Grant necessary authority to the IRT.

The 7 steps of preparation

- **Selection of IRT**
  - 2 sub-teams:
    1) Command Decision Team
    2) On-Site Incident Handling Team
  - Capacity & jurisdiction:
    - Local incident handling
  - Choose and organize beyond technical staff.
    – Include representatives from cross-functional units within organization,
  - Document IRT chart and members

The 7 steps of preparation

- **Selection of IRT:** Organizational Models for IRT
  - 1) Security Team
  - 2) Internal Distributed IRT
  - 3) Internal Centralized IRT
  - 4) Combined Distributed & Centralized IRT
  - 5) Coordinating IRT

- **Summary**
  - No single IRT model is perfect
  - Must be flexible enough to adapt to changes in IT landscape and different or emerging incident types
  - May shift model if necessary – not confined to one particular model
- All models require:
  - Adequate funding
  - Cooperation from functional units and members of the constituency
  - Point(s) of reporting contact
  - Active, open communication

The 7 steps of preparation

- **Communications Plan**
- Ensure contact lists are easily accessible to IRT.
  - Keep hard copies in off-site location
- Assign a scribe or note taker.
- Establish a primary point of contact(s)
  - e.g. Incident Command Center
- Have a plan for possible IRT staff overtime
  - Ordering food
  - Lodging (if necessary)
  - Shift changes

The 7 steps of preparation

- **Reporting Facilities**
  - User education program
    - New employee orientation
    - Yearly information security awareness briefing
- Help people recognize an incident
  - List of indicators
    - Easily accessible to everyone. e.g. intranet web site
  - Audience: end-users, customers, sys admins, IRT

The 7 steps of preparation

- **Reporting Facilities**
  - Establish and publish internal report channels.
    - Email address (abuse@...gr)
    - Phone numbers
    - Web form
    - Point-of-contact people with names

The 7 steps of preparation

- **Reporting Facilities**
  - Define incident parameters
    - – Requirements to be met before raising an alarm to senior management, business partners, and/or law enforcement agency
    - – ... for users, IT support staff, and IRT
    - – Requirements to escalate incident
      - Organizational policy violation,
      - legal compliance issue,
      - disruption of critical business service,
      - breach of legal obligation,
      - criminal activity,
      - etc.

The 7 steps of preparation

- **Train IRT**
  - Discuss how to handle different types of incident:
    - – Virus/worm epidemic
    - – Unauthorized access attempt
    - – Successful intrusion
      - Theft or exposure of institutional or private data
      - Network asset compromise
  - Discovery of illegal activity
    - e.g. personal commerce using employer's resource(s), child pornography, etc.
  - Write scenarios into formal IR plan.

The 7 steps of preparation

- **Train IRT**
  - Train / study log management
    - – How to secure system logs
    - – How to interpret logs
    - – Make sure to back up logs
  - Prepare and train IR & forensic tools

    – IR & forensic tools on read-only media

    – Blank media for forensic evidence collection/acquisition

    - Own a Security Incident Response & Forensic (SIRF) Toolkit

The 7 steps of preparation

- **Guidelines for Inter-departmental and peer cooperation**
  - Minor incidents:
    - Encourage handling by local IT support staff
    - e.g. virus infections
  - Utilize help desk:
    - First line of defense and reporting channel
    - Should be a part of IRT
    - Report trends to IRT
  - Offer workshops / cross-training sessions
  - “Reward”
    - Recognize those who discover an incident (or event that lead to discovery).
  - • Let peers / partners know about your IRT and IR procedures.

The 7 steps of preparation

- **Guidelines for Inter-departmental and peer cooperation**
  - Minor incidents:
    - Encourage handling by local IT support staff
    - e.g. virus infections
  - Utilize help desk:
    - First line of defense and reporting channel
    - Should be a part of IRT
    - Report trends to IRT
  - Offer workshops / cross-training sessions
  - “Reward”
    - Recognize those who discover an incident (or event that lead to discovery).
  - • Let peers / partners know about your IRT and IR procedures.

5. Six Phase Approach

- **Incident Handling Strategy**

  - 2. Identification
    - Who does what and how? Where is XYZ?
    - Assessment of situation.

5. Six Phase Approach: Identification

- **5 Steps**
  - **1. Assign an incident owner to the incident.**
  - **2. Determine whether it is really an incident**
  - **3. Maintain a chain of custody.**
  - **4. Coordinate actions.**
  - **5. Inform parties.**

5. Six Phase Approach: Identification

- **Assign an incident owner to the incident**
  - **Consider:**
    - **Handler's**
      - **general knowledge of enterprise or local site**
      - **familiarity with security policies and procedures**
      - **experience**
    - **Time of response: off-hours, weekend, holidays, etc.**
    - **Pool of potential handlers**

!Critical develop an Incident log!

5. Six Phase Approach: Identification

- **Determine Incident Nature**
  - **Is it really a security incident?**
    - **– False positive (by IDS)?**
    - **– Errors/bugs in system?**
    - **– Human mistake?**
  - **Talk to “witnesses” first.**
    - **– Sys admins**
    - **– Affected user(s)**
  - **Determine type of incident.**

!Critical develop an Incident log!

5. Six Phase Approach: Identification

- **Chain of Custody**
  - **Identify and collect evidence**
    - **Document when and how evidence is/was collected.**
    - **Document tools used to collect evidence with usage time stamps**
    - **Collect as much as possible. Determine relevancy later.**
      - **– Example: Backup tapes predate the incident!**
      - **– Label or document evidence.**
  - **Turn over evidence to next person in chain of custody**
    - **– i.e. forensic analyst**
  - Report to Command Decision Team..

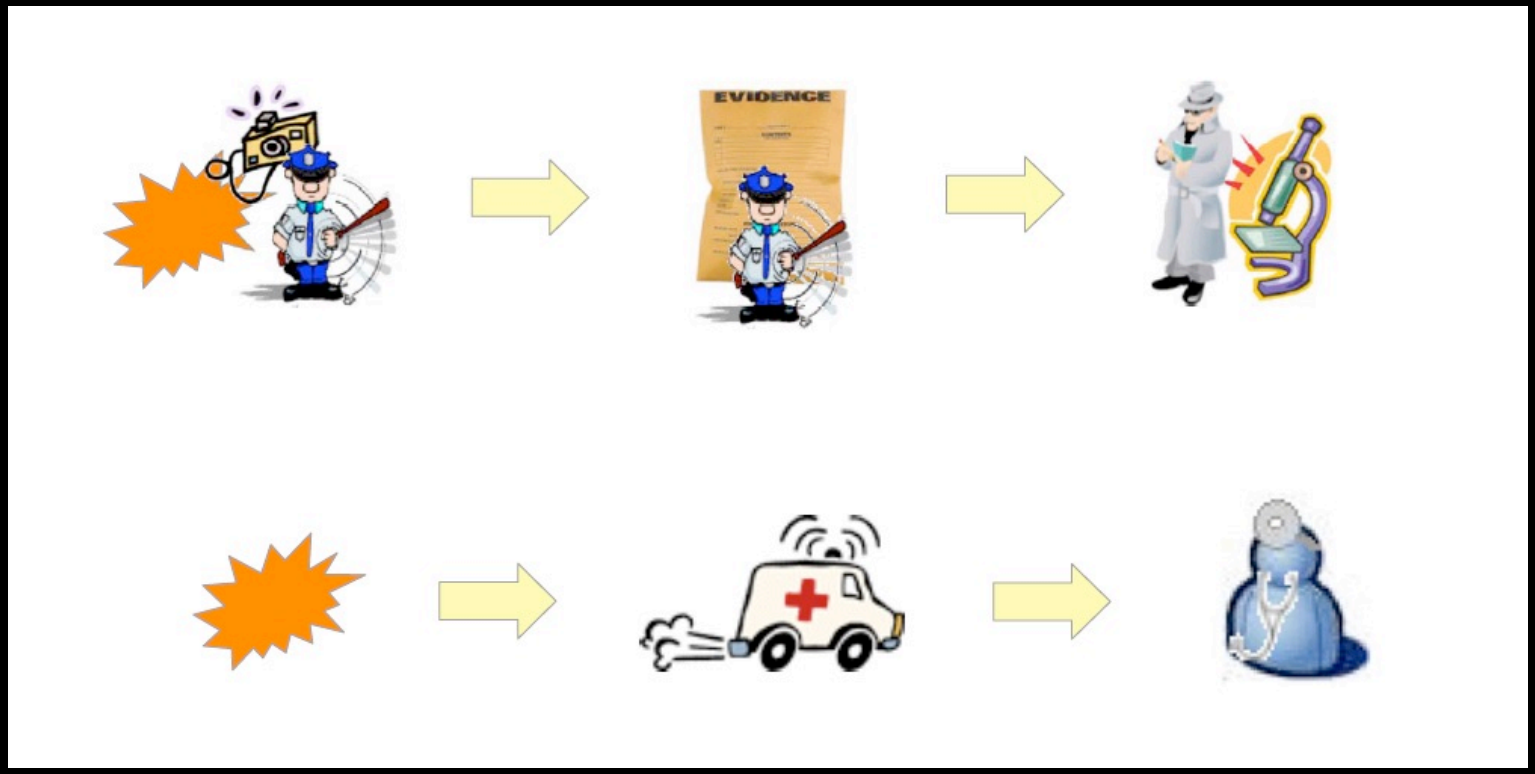
!Critical develop an Incident log!

5. Six Phase Approach: Identification

- **Chain of Custody**
  - **Identify and collect evidence**
    - **Document when and how evidence is/was collected.**
    - **Document tools used to collect evidence with usage time stamps**
    - **Collect as much as possible. Determine relevancy later.**
      - **– Example: Backup tapes predate the incident!**
      - **– Label or document evidence.**
  - **Turn over evidence to next person in chain of custody**
    - **– i.e. forensic analyst**
  - Report to Command Decision Team..

!Critical develop an Incident log!

Chain of Custody



Source: Univ. Buffalo

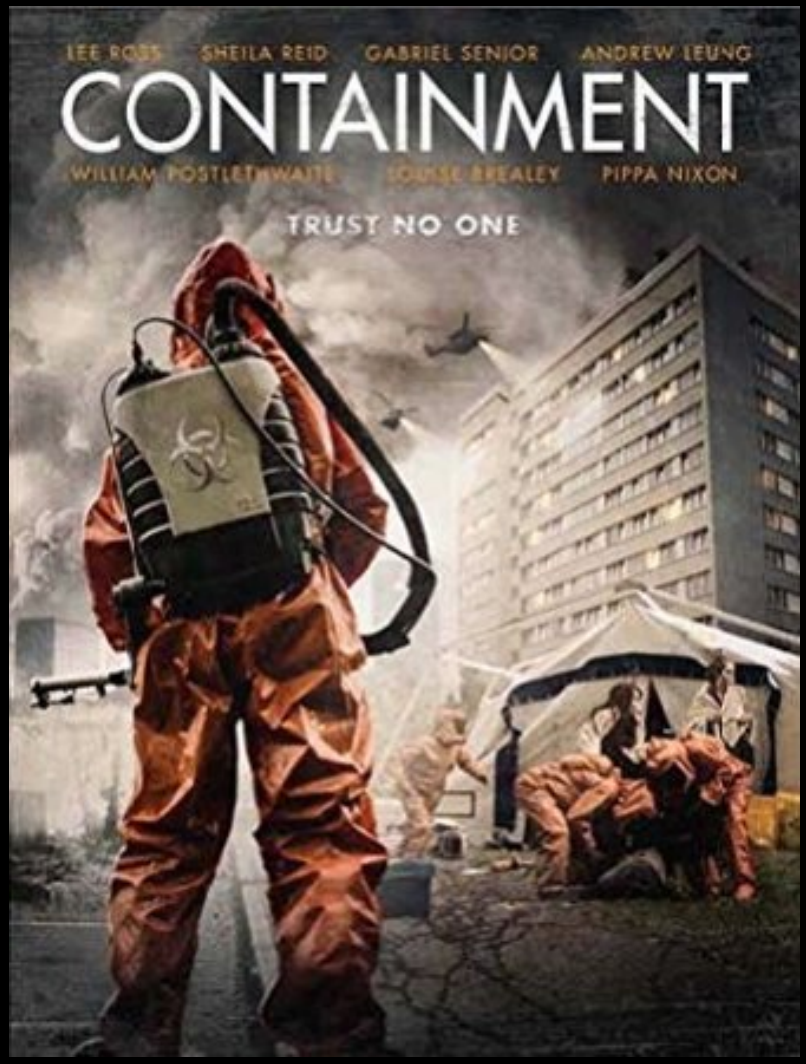
5. Six Phase Approach: Identification

- **Coordinate Actions**
  - **Delegate tasks to the rest of IRT members.**
  - **Involve IRT constituents in decision-makings.**
  - **Involve peer or external IRT if necessary.**

5. Six Phase Approach: Identification

- **Inform Parties**
  - **Notify all or relevant parts of organization.**
  - **Notify senior management and/or external entities in accordance with the incident parameters defined.**
  - **(See Preparation phase – Reporting Facilities.)**
  - **Status updates every ___ hours.**

Next week


LEE ROSS
SHEILA REID
GABRIEL SENIOR
ANDREW LEUNG
CONTAINMENT
WILLIAM POSTLETHWAITE
LOUISE BEALEY
PIPPA NIXON
TRUST NO ONE