



Minnesota State Colleges & Universities

# Incident Handling

*Applied Risk Management*

September 2002

Information Technology Services

Minnesota State Colleges and Universities

# What is Incident Handling?

*Incident Handling is the management of Information Security Events*

# What is an Information Security Event?

*An Information Security event is:*

- *potential harm creating potential risk*
- *threats attempting to exploit vulnerabilities*
- *unexplained anomalous behavior*
- *tangible attacks upon assets*

# Typical Information Security Events

*daily occurrences worldwide*

- **Malicious code**
  - *Viruses, worms, and logic bombs*
- **Network scanning**
  - *Worldwide vulnerability reconnaissance*
- **Network penetration**
  - *Bypassing of perimeter security controls*
- **Host compromise**
  - *Unauthorized access/modification to host machines*
- **Denial of service**
  - *Shutdown/degradation of network services or devices*
- **Data compromise/theft**
  - *Unauthorized access to protected data assets*

# Incident Handling Strategies

*planning the process*

An Incident Handling strategy must be:

- **Proactive**
  - *Cognizant of the threat environment*
  - *Risk Minimizing*
- **Reactive**
  - *Anomaly detecting*
  - *Real-time responsive*
- **Forensic**
  - *Post mortem analytic*
  - *Adaptive to lessons learned*

# Event Management Process

*implementation of the strategy*

Event management is a 5 step process

1. Preparation
2. Detection
3. Containment
4. Eradication
5. Evaluation

# Step 1: Preparation

know thy enemy

- **Risk Assessment**
  - *Understand the threat environment*
- **Risk mitigation**
  - *Deploy controls*
  - *Minimize exposure*
- **Education**
  - *Raise threat awareness*
  - *Publicize event reporting duties and procedures*

# Step 2: Detection

the hand in the cookie jar

- Real-time detection
  - *Network sniffing*
  - *Host monitoring*
- Forensic detection
  - *File checking*
  - *Log analysis*

# Step 3: Containment

*circle the wagons*

- **Networks**
  - *Affected segments are physically/logically isolated*
- **Hosts**
  - *Affected hosts are physically/logically isolated*
- **Data**
  - *Contaminated data is segregated*

# Step 4: Eradication

*cyber pest control*

- **Anomaly analysis**
  - *Determination of the root cause*
- **Cleansing**
  - *Removal of the wicked*
  - *Plugging of the leaks*
- **Restoration**
  - *Business continuity*

# Step 5: Evaluation

*fool me once, shame on you*

- Lessons learned
  - *Security re-evaluation*
- Information sharing
  - MnCERT
    - *Minnesota Computer Emergency Response Team*
  - FIRST
    - *Forum of Incident Response and Security Teams*

# Process Implementation

*making this all happen*

- **Intrusion detection**
  - *Sensors in various form monitor assets for anomalous events.*
- **Incident response**
  - *Triggers are activated when predefined anomaly thresholds are detected by sensors.*
  - *Responders react to trigger activation, following procedures to manage the event.*

# Process Implementation: Sensors

*commensurate with value of asset protected*

Sensors might include:

- **Educated employees**
  - *Eyes and ears to report suspicious activity*
- **Network based IDS**
  - *Network packet sniffing and signature analysis*
- **Host based IDS**
  - *Server process and port monitoring*
- **File integrity checkers**
  - *Baseline file comparators*
- **Log Analyzers**
  - *Logfile analyzer and reporting utilities*

# Process Implementation: Triggers

## *false positives versus false negatives*

Triggers must be tuned to capture events yet minimize false alarms:

- **Employee reports**
  - *First responder filters and triage*
- **Signature matches**
  - *Signature files must remain current*
- **Penetration attempts**
  - *Valid users, processes, and ports must be known*
- **Modified files**
  - *Valid baseline files must be maintained*
- **Log anomalies**
  - *Logfiles must be tamperproof*

# Process Implementation: Responders

*damage control and business restoration*

Responders must have the following:

- **Personnel**
  - *Multi-disciplinary skill sets*
- **Authorizations**
  - *Ability to react in a timely fashion*
- **Rosters**
  - *The enemy never sleeps*
- **Tools**
  - *Specialized toolkits must be assembled, tested, and deployed*
- **Procedures**
  - *Procedures must be created, and tested*

# Responders: Personnel

## *The Incident Response Team*

Personnel included in an IRT might include:

- Incident Commander ( IC )
  - *Oversee and manage the mayhem*
- Dogfighters
  - *LAN/WAN administrators/engineers*
    - Skilled in IP routing and trace-back
  - *Host administrators/engineers*
    - Skilled in relevant operating systems analysis and restoration
- Legal
  - *Oversee chain of custody issues*

# Responders: Personnel

## *The Incident Response Team*

- Public Relations
  - *Present “official line” to media inquiries*
- Human Resources
  - *When suspicion points internally*
- Law enforcement liaisons
  - *When your event proves to be the tip of the iceberg*

# Responders: Authorizations

*tactical decision making*

It is crucial that responders have unquestioned authority to:

- **Stop network connections**
  - *May be the best or only way to repair damage*
  - *Your network may be the source of someone else's "event"*
- **Isolate host machines**
  - *Host machine may be "owned" by another*
  - *Isolation may allow effective purging and reconstruction*

In both cases, the resultant **denial of service** should be considered in a security risk assessment. Redundancy should be integral to the architecture as required.

# Responders: Rosters

*attacks know no boundaries*

## Issues to consider in staffing

- Rotation policy
  - *24X7 coverage*
  - *Incentives*
- Communication channels
  - *Pagers*
  - *Remote access*

# Responders: Tools

- **Accurate infrastructure diagrams**
  - *Crucial to tracing event flow*
- **Network scanners**
  - *Catching the action in real-time*
- **Network device configuration backups**
  - *Restoration of operations*
- **Host backups**
  - *Restoration of services*

# Responders: Tools

- **Disk mirroring tools**
  - *Post mortem analysis*
  - *Legal evidence*
- **Log books**
  - *Post mortem analysis*
  - *Legal evidence*
- **Out of band communications**
  - *Secure communications channel*

# Responders: Procedures

*step by step methodologies*

- Creative thinking should be encouraged
  - *Think like the enemy*
- Procedures should be flexible
  - *Dogfighters must be able to adapt to changing threats*
- Procedures correspond to event categories
  - *Each requires unique skill sets and responses*
- Procedures address incident stages
  - *From discovery to persecution of the innocent*

# Event categories and stages

## Event categories

- **Malicious code**
  - Virus / worms
- **Infrastructure reconnaissance**
  - Probes / scans
- **Network penetration**
  - circumvention of perimeter security
- **Device compromise**
  - Unauthorized configuration changes
- **Denial of service**
  - Shutdown of services
- **Data exposure / theft**
  - Breach of confidentiality

## Incident stages

- **Cold**
  - No threat detected
- **Warm**
  - Trigger activated
  - Resources mobilized
- **Hot**
  - Attack in progress
    - Containment
    - Eradication
    - Restoration
- **Cool-down**
  - Event Analysis

# Incident Handling Recap

- **Know the threat**
  - Security Risk Assessment
- **Create strategy**
  - Proactive
  - Reactive
  - Forensic
- **Deploy sensors**
  - Cost justify
  - Balance false positive and false negatives
- **Create Response mechanisms**
  - Teams
  - Tools
  - Procedures

# Incident Handling Benefits

*Incident handling is key to any Information Security Program*

A coherent incident handling strategy

- *Documents due diligence*

An effective event management process

- *Promotes mission continuity*
- *Enhances enterprise image and reputation*