NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Incident Response Planning

Nicholas Santora, CISSP, CISA
CIP Cybersecurity Specialist , NERC

RELIABILITY | ACCOUNTABILITY




Agenda

- PICERL Process
- Where is your Incident Response Program?
- What is a V5 Cyber Security Incident?
- How this fits in to CIP-008-5
- Tools and Guidance
- Questions

PICERL

- Start Simple!
- Don’t let process absorb functionality
- PICERL
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned

1) Preparation

- Planning is everything
- Management support
- Policy Review
  - Ensure permission from system owner exists
    - Monitor traffic
    - Monitor employees
    - Review hard drives
  - No expectation of privacy

1) Preparation

- Law Enforcement interaction
- Tracking
  - Helpdesk system
  - Incident Response system
  - Notepads (seriously!)

1) Preparation

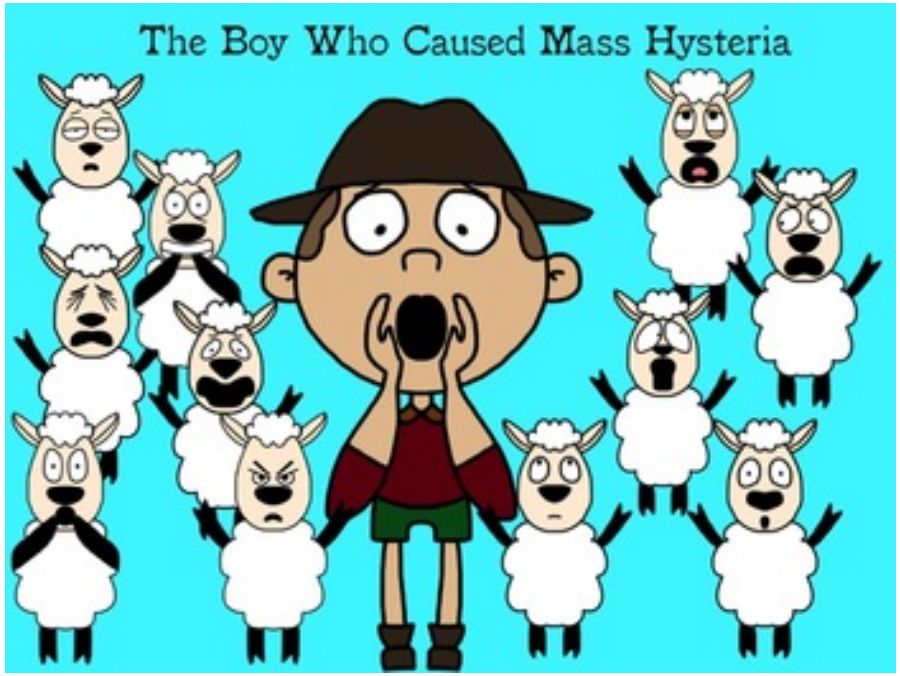
- Identify your team
  - Not everyone is a great incident handler
  - Stressful
  - Available at “best times!”
- Turn users into an alert system
  - This is what awareness is all about

1) Preparation

- Think about an “IRP jump kit”
  - Disaster Recovery Plan (short term)
  - Checklists
  - Procedures
  - Emergency Comms Plan
  - Other tools
  - Password escrows/keys

2) Identification

- Alert of an incident
- How to define an incident?
- Have trained individuals analyze
- Goal: Not Be Boy Who Cried Wolf!
  - Control Room example



2) Identification

- How do you know an incident took place?
  - Where did alert originate?
  - Who did it come from?
  - Who to talk to?
- Who makes the decision?
  - Involve Senior Management
  - Need to Know
  - Media

2) Identification

- Assign a primary handler
- Checklist for first responders
  - Date
  - Time
  - Description
  - First sign
  - Patterns

3) Containment

- Do not make things worse! Make Better!
- Isolating the issue
- Document what is or will be done
- Understand basic principals of liability and negligence
- Not just about pulling the plug
- Making backups

4) Eradication

- Understanding the scope of the problem
- Fix before putting back online
  - Nuke the OS
  - Manual cleanup

- Identifying the attack vector!

4) Eradication

- What about my production system?
  - If compromised, it has a vulnerability
  - Potential for compromise again
- Perform any other cleanup needed
  - Change name
  - IP address
  - Integrity check
  - Additional scans

5) Recovery

- Bring systems back to normal conditions
- Do NOT restore compromised code
  - Use tools upon restore for integrity checks
- Validate the system
- System owner makes call on full operation
  - They depend on the system
- MONITOR!

6) Lessons Learned

- Most important and underappreciated step
- Learn from your mistakes
- Gather all related information and facts
- Have on-site handler submit draft exec summary

6) Lessons Learned

- Bring in outside points of view (non-technical)
- People are tired and stressed
- Analyze which controls are working and which are not
  - Focus on improvement not blame

Definitions (CIP-008-5)

- **Cyber Security Incident**: "A malicious act or suspicious event that:
  - Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or,
  - Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.
- **Reportable Cyber Security Incident:** "A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity."

- One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law.
- Must be within 1 hour when discovered
- Test every 15 months
- Document deviations from the plan in exercise
- Document lessons learned within 90 days

Resources

- SANS Internet Storm Center
- PacketStorm.org
- BugTraq
- National Vulnerability Database
- ES-ISAC
- Infragaurd

Wrap up

- Take a look at the PICERL Process
- Keep your process simple
- Lessons learned are VERY important
- Continuous testing

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions

Nicholas Santora, CISSP, CISA
CIP Cybersecurity Specialist, NERC

RELIABILITY | ACCOUNTABILITY