# Incident Response 100

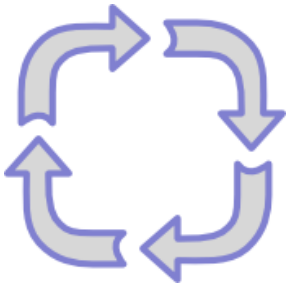
*Building an incident response capability*

Layerone Conference , May 2009

Ryan S. Upton, CISSP

# Introduction

**Establish the Incident Response Program**



**Form the Plan and Processes**

**Improve the Program**

## *Prepare & Establish*

- Find a balance between Responsibility and Authority
- Set Expectations with Executives
- Create a Draft Plan
- Identify your resources
- Get your approval / charter / whatever

## *Incident Response Phases:*

0) **Preparation**

1) **Triage**

2) **Containment**

3) **Response**

4) **Resolution**

# *Roles:*

**Roles are not people.**

- **Incident Coordinator**
- **Incident Manager(s)**
- **Incident Responder(s)**
- **Subject Matter Experts - SME's**
- **The hammer of God.**

**Separate Management and Coordination roles from responders.**

## *Resource Management*

- Staff
- Skill sets and Training
- Consultants
- Budget
- Time

# *Communication:*

- Build relationships
  - legal & forensics response teams
  - Press/PR
  - Executive/board
  - HR – HR, and ... HR
  - Physical security and Safety groups
  - Audit department
  - Fraud department
  - Business Relationship management
  - IT Operations (if this isn't you already)
  - Regulatory Compliance office
  - Highly involved Management (Office of COO, or whoever can shake trees and will want to know status and conclusion).
  - BCP/DR – let's hope you don't need them.
  - Business risk managers; In addition to clear business insight and industry/ process knowledge believe it or not, some companies buy hacker insurance- and to collect they need well documented information and details..
  - Externally:
    - industry info sharing groups (EG: ISAC's)
    - Consulting companies (bulk forensics response, etc)

## *Sensitive Issues*

- Incident Response is NEED TO KNOW.
- Establish how an issue becomes an Incident
- Establish handling in process, training and tests.
- Don't idly chat- you need the time anyway.

## *Maturity Model*

0. **Informal**
1. **Documented**
2. **Established**
3. **Tested**
4. **Integrated**
5. **Acculturated**

# *Final Thoughts*

- **Keep an eye on “Why”.**
- **It's not all about you.**
- **Work to Completion.**
- **Re-use stuff that works!**

# The End
# (Q&A)

*Thanks for your interest.*

Contact:
Ryan S. Upton
ryanu@pobox.com

Resources:

- ISC SANS Handlers Diaries *(too many to list)*
- NIST “Computer Security Incident Handling Guide” (800-061)
- American Institute of Certified Public Accountants (AICPA.org) Incident Response Plan