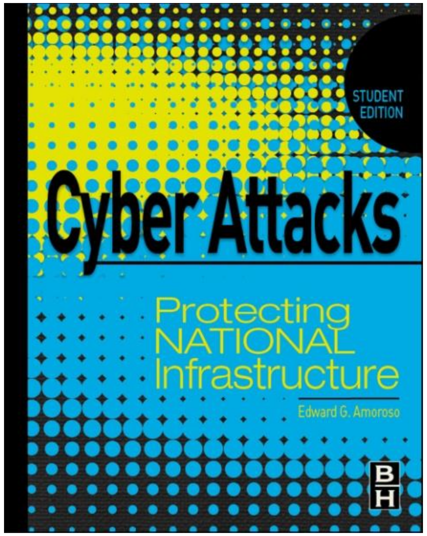


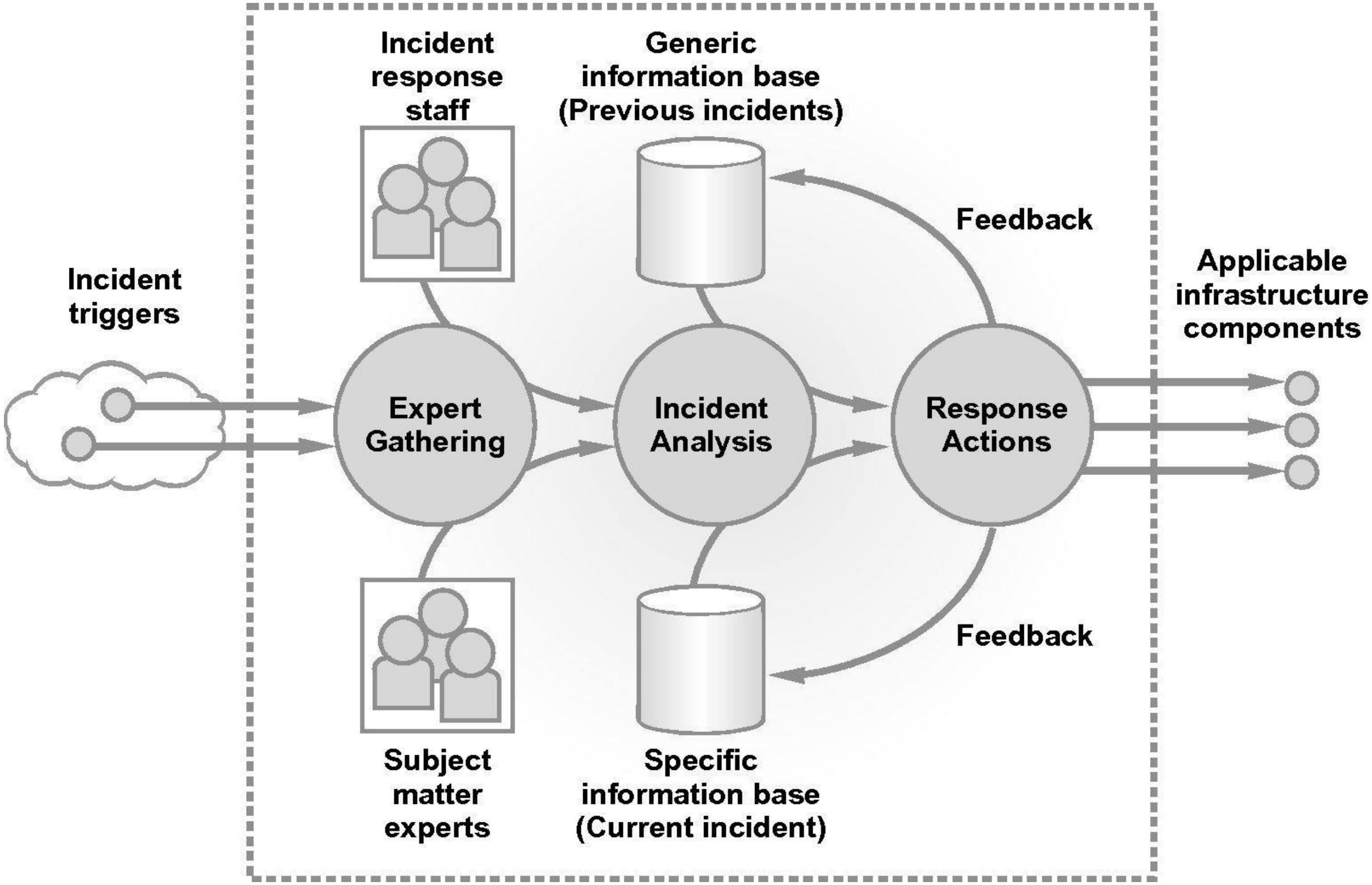
Chapter 11

Response

Introduction

- Incident response process is the most familiar component of any cyber security program
- A cyber security program will contain at least the following
  - Incident trigger
  - Expert gathering
  - Incident analysis
  - Response activities

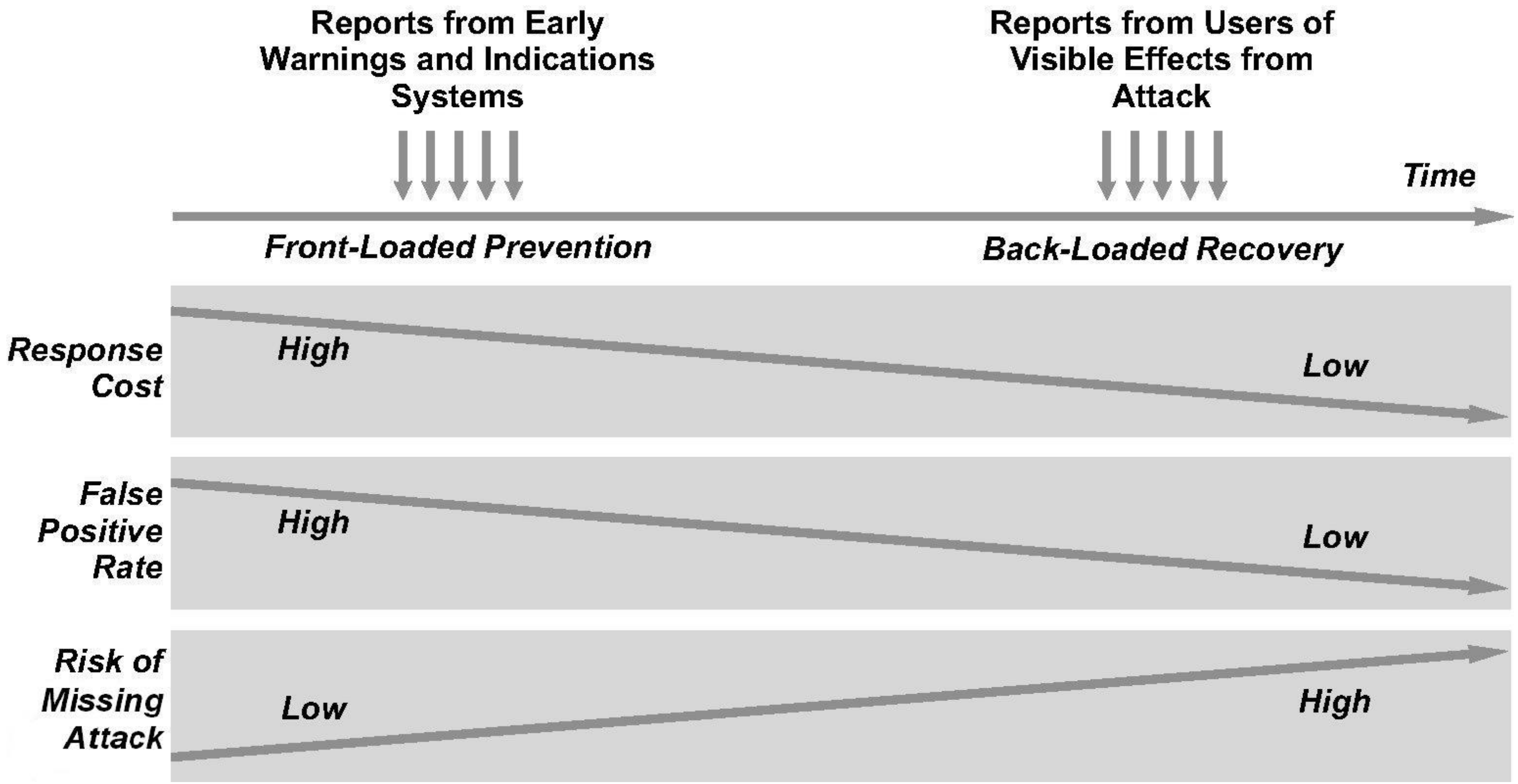
Fig. 11.1 – General incident response process schema



Pre- Versus Post-Attack Response

- There are two fundamental types of triggers
  - Tangible, visible effects of an attack
  - Early warning and indications information
- Thus, two approaches to incident response processes
  - Front-loaded prevention
  - Back-loaded recovery
- The two approaches should be combined for comprehensive response picture
- Protecting national assets is worth suffering a high number of false positives

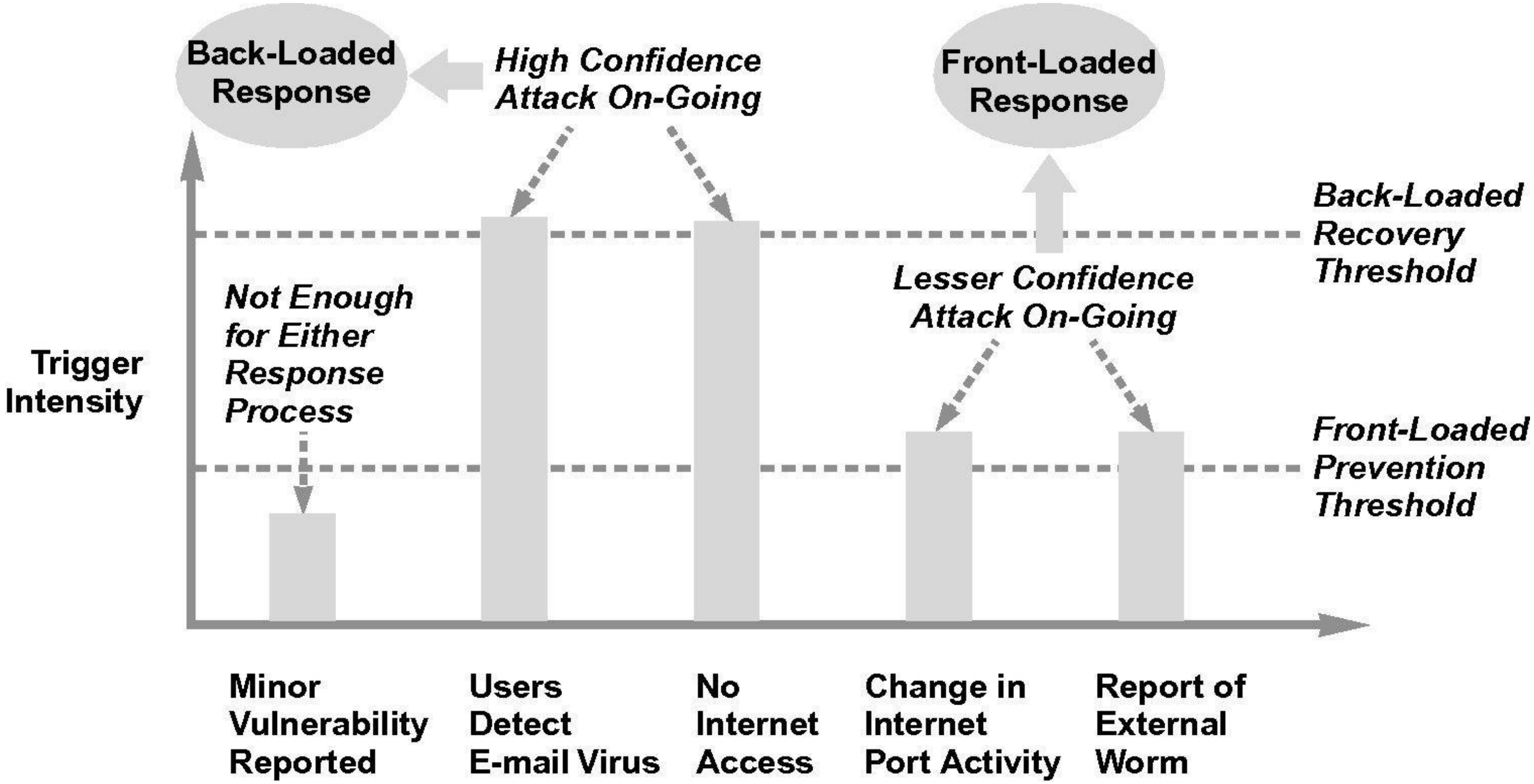
Fig. 11.2 – Comparison of front-loaded and back-loaded response processes



Indications and Warning

- Front-loaded prevention critical to national infrastructure protection
- Taxonomy of early warning process triggers
  - Vulnerability information
  - Changes in profiled behavioral metrics
  - Match on attack metric pattern
  - Component anomalies
  - External attack information
- Front-loaded prevention have a high sensitivity to triggers

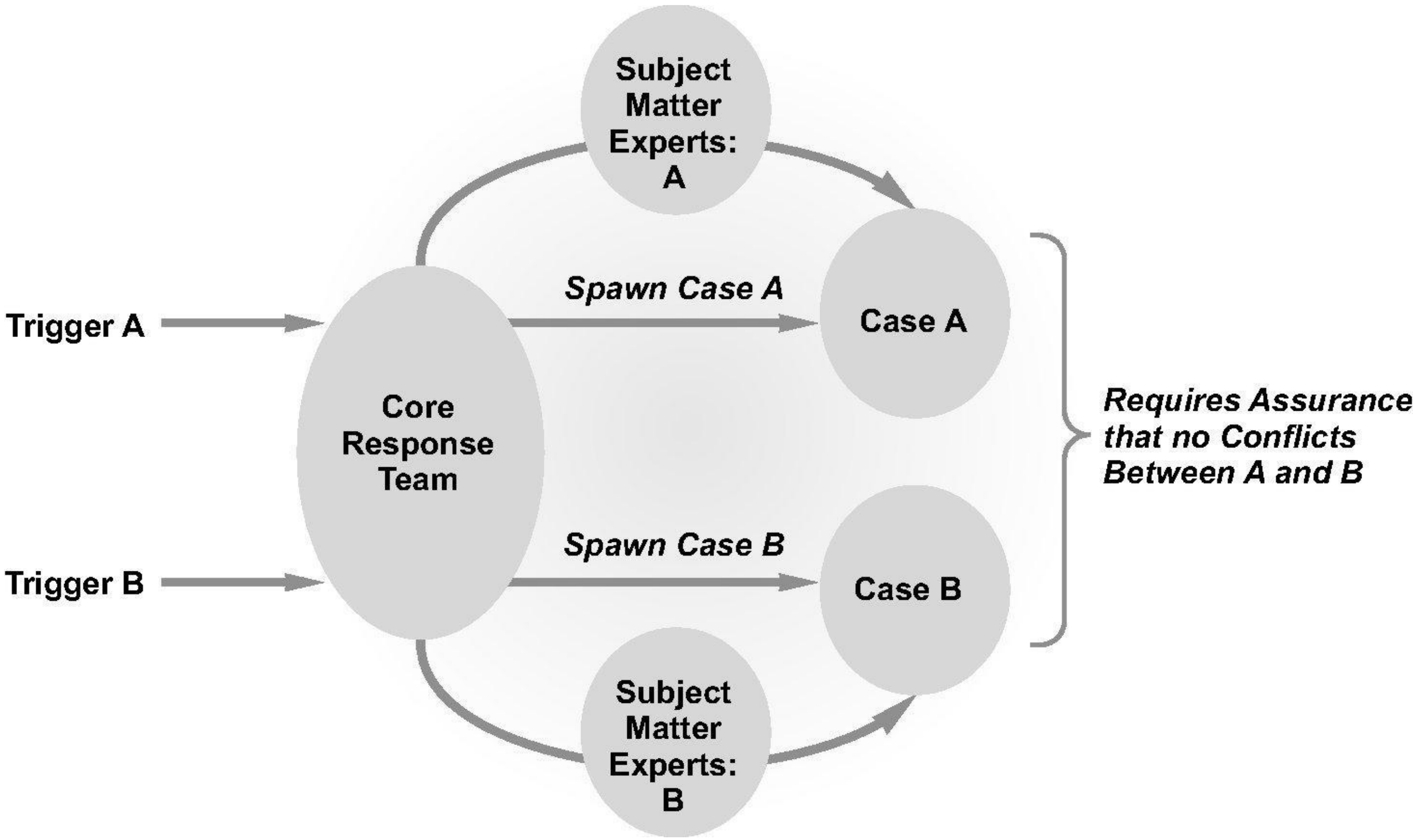
Fig. 11.3 – Comparison of trigger intensity threshold for response


Back-Loaded Response
High Confidence Attack On-Going
Front-Loaded Response
Back-Loaded Recovery Threshold
Lesser Confidence Attack On-Going
Not Enough for Either Response Process
Trigger Intensity
Front-Loaded Prevention Threshold
Minor Vulnerability Reported
Users Detect E-mail Virus
No Internet Access
Change in Internet Port Activity
Report of External Worm

Incident Response Teams

- Optimal incident response team includes two components
  - A core set of individuals
  - A set of subject matter experts
- In complex settings, with multiple incidents, important for team to not work at cross-purposes

Fig. 11.4 – Management of simultaneous response cases


Subject Matter Experts: A
Trigger A
Spawn Case A
Case A
Core Response Team
Requires Assurance that no Conflicts Between A and B
Trigger B
Spawn Case B
Case B
Subject Matter Experts: B

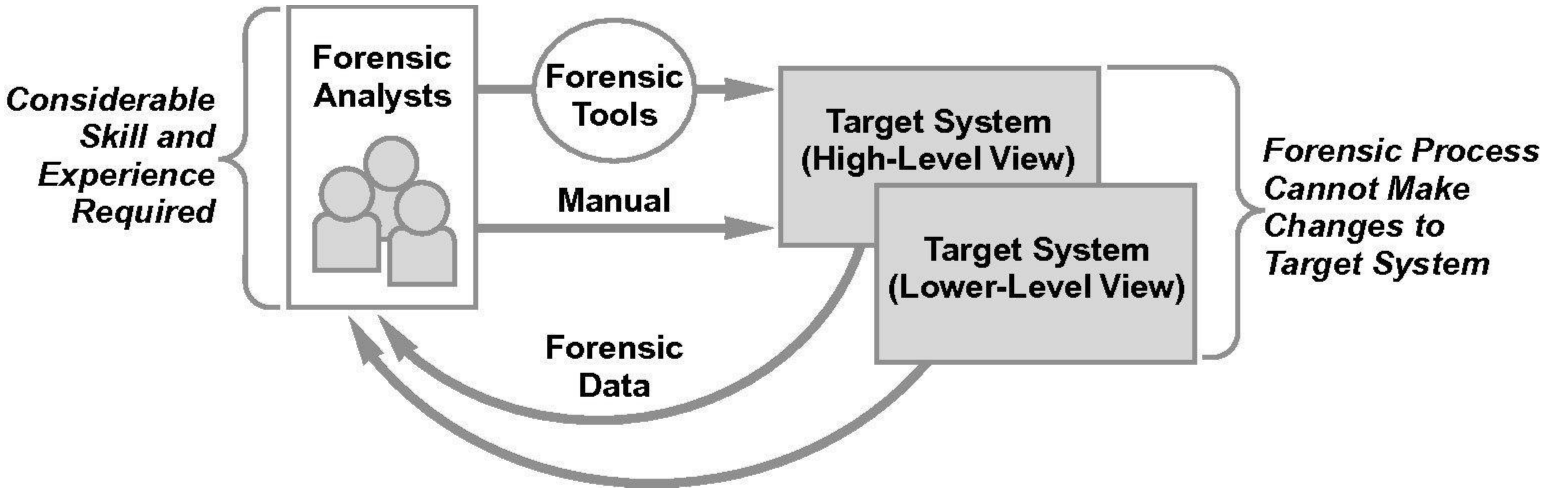
Incident Response Teams

- Response teams in a national setting must plan for multiple concurrent attacks aimed at a company or agency
- Considerations for proper planning include
  - Avoidance of a single point of contact individual
  - Case management automation
  - Organizational support for expert involvement
  - 24/7 operational support

Forensic Analysis

- Questions addressed in the forensic analysis process include
  - Root cause
  - Exploits
  - State
  - Consequences
  - Action
- Great care must be taken to protect and preserve evidence

Fig. 11.5 – Generic high-level forensic process schema


Considerable Skill and Experience Required
Forensic Analysts
Forensic Tools
Manual
Target System (High-Level View)
Target System (Lower-Level View)
Forensic Data
Forensic Process Cannot Make Changes to Target System

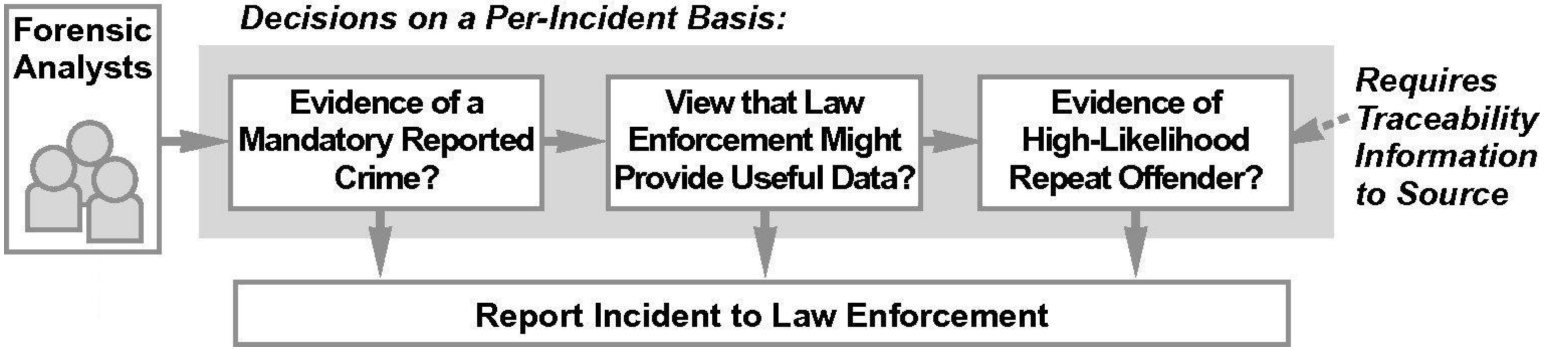
Forensic Analysis

- Internal expert most likely the best to lead a company investigation
- Forensic analysts need the following
  - Culture of relative freedom
  - Access to interesting technology
  - Ability to interact externally

Law Enforcement Issues

- Should law enforcement be involved and called upon for support?
- Carefully review local, regional, and national laws regarding when law enforcement *must* be contacted
- Figure 11.6 outlines a decision process

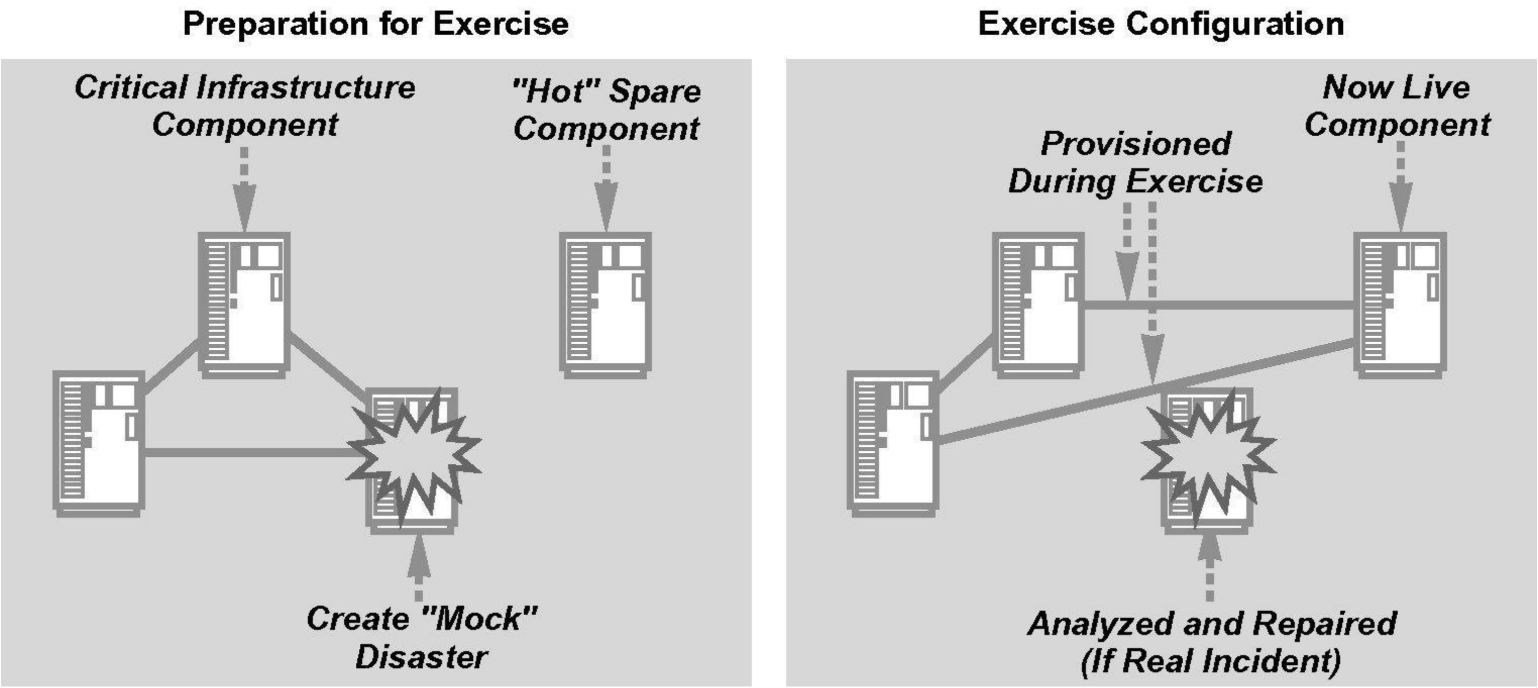
Fig. 11.6 – Decision process for law enforcement involvement in forensics


Forensic Analysts
Decisions on a Per-Incident Basis:
Evidence of a Mandatory Reported Crime?
View that Law Enforcement Might Provide Useful Data?
Evidence of High-Likelihood Repeat Offender?
Requires Traceability Information to Source
Report Incident to Law Enforcement

Disaster Recovery

- Three Components of a Disaster Recovery Program
    - Preparation
    - Planning
    - Practice

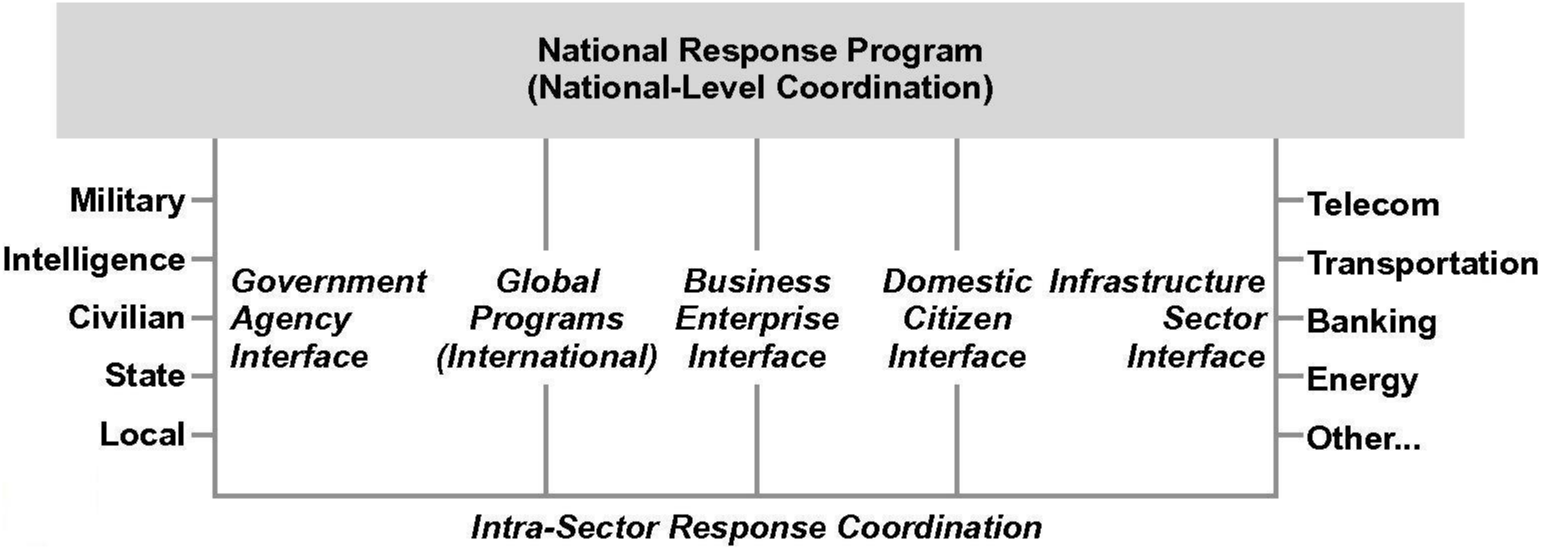
Fig. 11.7 – Disaster recovery exercise configurations



National Response Program

- National programs can provide centralized coordination
  - Intrasector coordination should be encouraged
- Currently, coordination is not the main focus of most national emergency response team programs

Fig. 11.8 – National response program coordination interfaces


National Response Program
(National-Level Coordination)
Military
Intelligence
Civilian
State
Local
Government Agency Interface
Global Programs (International)
Business Enterprise Interface
Domestic Citizen Interface
Infrastructure Sector Interface
Telecom
Transportation
Banking
Energy
Other...
Intra-Sector Response Coordination