Railroad Infrastructure Security

TRB Annual Meeting
January 14, 2002
Session 107 - Railroad Security

William C. Thompson
william.thompson@jacobs.com
402-697-5011
Railroad Infrastructure Security

Thanks to:

Bob Ulrich
Dr. William Harris
Byron Ratcliff
Frank Thigpen
John Ross
George Biedenbender
Railroad Infrastructure Security

Creating awareness of security issues

- Railroad History
- Incident Handling Process
- Considerations when updating your emergency response plan
  - Threats and Mitigation of Other Risks
- Countermeasure Study and Research Needs
Railroad Infrastructure Security

Railroads and Natural Disasters

- In their 175+ years of operation, US railroads have encountered many natural disasters that have damaged or destroyed track and equipment
  - Snow & Ice Storms
  - Floods
  - Landslides
  - Earthquakes
  - Hurricanes & Tornadoes
Railroad Response to Natural Disasters

- Developed staff and equipment capabilities to deal with natural disasters
- Established opportunities for contractors to augment their internal staff
- Negotiated agreements to carry trains of competitive railroads under agreed conditions in case of line blockage
Railroad Infrastructure Security

• Railroads and Hazmat
  – Major carriers of hazardous materials
  – Crews are trained in response to hazmat releases in accidents
  – Have protocols in place to call on shippers of hazmat and consignees to augment their staff in controlling and clean up after releases
Railroad Infrastructure Security

- Railroads and Criminal Attacks
  - Train robberies were once common
  - Railroads established police forces with independent police authority and with provisions for cooperation with government law enforcement offices
  - Criminal acts against railroads are rare
Railroad Infrastructure Security

• Reasons for Attacks on Railroads
  – Terrorists may seek to endanger the population by attacking trains carrying hazardous or nuclear materials
  – Terrorists may seek to disrupt essential governmental shipments of military equipment by attacking trains or routes essential to that traffic
  – Terrorists may seek to disrupt the US economy by disrupting commercially essential shipments
Railroad Infrastructure Security

How can Terrorists Attack Railroads

- Railroad tracks and switches are vulnerable to attacks by unbolting of joint bars or misalignment of switches
- Railroad bridges are vulnerable to attack by explosives
- Railroad tunnels are vulnerable to attacks by explosives and chem-bio agents
- Railroad control and dispatching systems are vulnerable to explosive and to cyber attacks
Railroad Infrastructure Security

- Railroad Response to Terrorists
  - Increase awareness of railroad management and employees to vulnerabilities and training of responders
  - Increase surveillance of critical assets
  - Seek inputs from government agencies on threats and responses to threats
  - Take appropriate measures to share information between railroads as through Information Sharing and Analysis Centers
Railroad Infrastructure Security

- Railroad Incident Response Process
  - Notification & secure site
  - Advise management
  - First step backwards
    - Check haz-mat
    - Employee and public exposure
  - Send in investigation team
    - Determine root cause *
  - Clean-up
  - Return to service
Railroad Infrastructure Security

- Derailment Investigation Process (SOP)
  - Safety first
  - Train, track & crew documentation
  - Drug testing and interviews
  - Site sketch, drawings or video
  - Event recorder evaluation
  - Determine point of derailment
  - Determine first car derailed
  - Analysis
  - Determine cause
Railroad Infrastructure Security

- Continuous Improvement (also Quality Process or PDCA)
  - Identification
  - Analysis
  - Determine alternative solutions
  - Develop solutions
  - Implementation
  - Evaluation
Critical Lesson Learned:

Everybody involved in the management, investigation and cleanup of the incident must communicate clearly and absolutely ensure that each correctly understands the other. Effective and precise communication is critical to minimizing further risk.
Railroad Infrastructure Security

- Considerations when updating your emergency response plan

  - Following can be used as a checklist
Railroad Infrastructure Security

Threat Assessment

Vulnerability Analysis

Risk Management Decision

Security Countermeasures
Railroad Infrastructure Security

• Threat Assessment
  – At what level are we operating?
    • Low
    • Moderate
    • Significant
    • High
Railroad Infrastructure Security

- Assessment Process
  - Awareness is key
Railroad Infrastructure Security

- Threat Assessment
  - From whom do you get your threat information?
  - How do you disseminate the information?
  - Exactly what does the information mean?
  - Evaluate the Source
  - Categorize the information
  - Prioritize
Railroad Infrastructure Security

- Vulnerability Assessment
  - Who?
    - What?
      - When?
        - Where?
          - How?

As related to the railroad or transit.
Railroad Infrastructure Security

- Assessment Process
  - Who can be called a legitimate threat?
    - Disgruntled employees, vendors or contractors
    - Disaffected individuals
    - Individual with intent to commit a felony
Railroad Infrastructure Security

• Assessment Process
  – What are areas of maximum regret?
    • Mass Casualties
    • Facility Failure
    • Medium to long term denial of service
Railroad Infrastructure Security

• Assessment Process
  – When are your assets most vulnerable
  – Identify your most critical assets
  – Level of control/interface with external infrastructure
  – Interactions
Railroad Infrastructure Security

- Availability of Friendly Forces
  - Internal security forces?
  - Coordination with federal, state and local authorities?
  - Coordination with contractors?
  - Coordination with on-call experts?
  - Do you have a plan in place that can be activated immediately?
  - Command and Response Structure in place
Railroad Infrastructure Security

- How can a threat be carried out against your critical assets
  - What assets do you control?
  - What are your redundant assets?
  - What is the status of your detection and sensor systems?
Railroad Infrastructure Security

• Risk Management Decisions
  – What is the threat?
  – Where are you vulnerable?
  – What type of countermeasures are deployed?
  – Who will deploy?
  – Who is in control?
  – Does everyone involved understand what is being communicated?
Railroad Infrastructure Security

- Risk Management Decisions
  - Primary Objectives
    - Prevent casualties
    - Ensure integrity of assets
    - Provide for continued operations
    - Reduce costs
Railroad Infrastructure Security

- Risk Management Decisions
  - Assess countermeasures in place
    - How is police or internal security force trained, organized and equipped?
    - How is security force deployed?
    - Do you have a central communications and command system in place?
Railroad Infrastructure Security

• Risk Management Decisions
  – Is your response plan coordinated among all friendly forces?
  – Does your response plan have redundancies in systems, procedures and processes?
  – Does your response plan allow for changes in threat level?
Railroad Infrastructure Security

- Security Countermeasures
  - Systems and plans must be designed to:
    - Deter
    - Detect
    - Delay
    - Deny / defend
    - Defeat
Railroad Infrastructure Security

- Security Countermeasures
  - Security Triad
    - Detection
    - Assessment
    - Response
Railroad Infrastructure Security

• Security Countermeasures
  – Detection
    • Human Assets
    • Electronic Assets
    • Canine Assets
Railroad Infrastructure Security

• Security Countermeasures
  – Assessment
    • Determine Extent of Incident
      – Single event vs. multiple attacks
      – Critical nature of event
      – How disruptive
    • Does your communication system allow you to make an assessment?
      – Have you tested under stress?
Railroad Infrastructure Security

- Security Countermeasures
  - Response and Reconstitution
    - Post incident mode
    - Accurate communication
    - Identified multiple evacuation routes
    - Established containment systems
    - Known roles and responsibilities
Railroad Infrastructure Security

- Security Countermeasures
  - Response and Reconstitution
    - Crisis management plans in place
    - Consensus building by all respondents
    - Interdependence of responding agencies
    - Preparedness drills
Railroad Infrastructure Security

Training

- An effort that must be accomplished
  - Unit level training
    - Individual level
    - Team level
    - Organizational level
  - Equipment training
    - Organizational
    - Equipment vendors
    - Outside organizations
Railroad Infrastructure Security

- Countermeasure Study and Research Needs
  - Staffing, planning and decision support
  - Real-time assessment, detection & warning
  - Systems analysis
    - Stability
    - Redundancy and system integration
  - Cross-functional impacts (cyber)
  - Personal protective equipment
  - Air handling systems
  - Decontamination