GLOBAL THREAT REDUCTION INITIATIVE

Subgroup Exercise 7, part 3

Task 1

Objective: Apply information from previous lectures and exercises to develop a more effective security system for the radioactive materials at UMC. The exercise will be conducted as a team (for each sub-group). It will perhaps be beneficial to the sub-group if they can divide the responsibilities contained in the tasks below to specific group members. The Sandia sub-group facilitator will provide assistance as requested but will otherwise only observe.

Threat: Assume a threat of two (2) persons, one of which is an active insider. The insider has knowledge, access and authorities appropriate for their job role and responsibilities. Limit the insiders to either: a guard, a radiation worker, a manager, or a member of housekeeping staff. The insider is either: bribed, disgruntled or coerced. If coerced, insider will not harm anyone. If bribed, insider will not harm co-workers. If disgruntled, insider will harm all. The outsider adversary is a criminal (or terrorist) desiring theft of radioactive material (or sabotage and release of radiation). Tools of the outsider are any tools than can be purchased by the public, a small utility van or truck, a handgun and/or hunting rifle, 20 kgs of TNT, and 200 grams of plastic explosive. The adversaries have knowledge and experience with the tools, weapons, and explosives.

Assumptions:

- Police can respond to UMC 7 minutes: 2 police officers in one car armed with handguns and one shotgun.
  - Adversary delay introduced by 2 police officers that deploy to interrupt adversaries is 45 seconds (once deployed).
- Follow up response to UMC in 5 minutes after call for backup (after 7 minute initial deployment + 3 minutes of assessment): 4 police officers in two cars, armed with handguns and one shot gun, one rifle.
- ARAS activated at 10 minutes from first call, deployment time is 20 minutes.
- Deployment time for police officers after arrival at UMC:
  - Police officers unfamiliar with the UMC facility layout and without a pre-developed, UMC-specific tactical plan.
    - 10 minutes
  - Police officers familiar with UMC facility layout and tactical plan.
    - 90 seconds
- If ARAS is deployed, tactical entry requires an additional 5 minutes after deployment to target area.

Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. . SAND# 2013-XXXXP

- Neutralization Success[1]:

# of Police Officers	Contain Adversaries at UMC perimeter (theft)	Contain Adversaries at source room (theft)	Tactical Entry & Neutralize 2 Adversaries (sabotage)
1	Very Low	Medium	Very Low
2	Low	High	Low
3	Low	Very High	Medium
4	Medium	Very High	High
5+	High	Very High	Very High

- Required effectiveness :
  - Both Detection (timely) and Neutralization effectiveness: High
    OR
  - Either Detection or Neutralization Effectiveness Medium, and other is Very High

Scenario 1:

A. Selecting either the Blood Center or Vivarium, brainstorm possible weaknesses in the UMC security system detection, access control, delay or response for a theft of radioactive material or the entire device.

B. Develop an adversary scenario (using the exercise 5 scenario as an example) to steal a radioactive source or entire device from the blood bank or Vivarium using the adversary threat defined above. Select an insider from the 4 categories, considering how the insider will be assist the scenario (minimize adversary detection, minimize scenario delay and task time, facilitate access control, perform malicious act (remove source), or minimize response effectiveness.

C. Estimate the adversary delay along the scenario path, and the points of possible detection, along with their likelihood (H, M, L) using data developed in exercises 3, 4 and 5. List equipment needed by adversary, along with weight. Estimate difficulty of tasks.

D. Employing response assumptions, estimate likelihood of security system effectiveness (i.e., estimate detection effectiveness and neutralization effectiveness) for the scenario.

E. Develop detection, assessment, access control, delay and/or response improvements to improve effectiveness.
   a. Address core weakness(es) that was exploited by adversary (e.g. lack of detection,

[1] The values in this tables are estimates for the purposes of the exercise and have no validity otherwise.

no assessment, lack of delay, weak access control, slow response…]

b. Consider improvements to decrease effectiveness of insider
c. Try to minimize cost of improvements
d. Try to minimize operational impact of improvements
e. Estimate detection and neutralization effectiveness and compare to requirement.

Scenario 1 Data

Insider selected and why: _____

_____

Target Facility and why: _____

_____

Adversary Scenario: Time of attack: _____

Adversary Equipment: _____

Steps/Path of Attack/Description/detection estimate/delay time:

1: _____

2: _____

3: _____

4: _____

5: _____

6: _____

7: _____

8: _____

9: _____

10: _____

Estimated Security Timely Detection Likelihood: _____

Estimated Neutralization Likelihood: _____

What is core weakness of security system against this scenario?

Detection: _____

Delay: _____

Response: _____

Planned Upgrades: _____

_____

_____

Upgraded Security Timely Detection Likelihood: _____

Upgraded Neutralization Likelihood: _____

Scenario 2:

A. Selecting either the Blood Center or Vivarium, brainstorm possible weaknesses in the UMC security system detection, access control, delay or response for a sabotage with radioactive release.
B. Develop an adversary scenario (using the exercise 5 scenario as an example) to sabotage in place the radioactive source(s) or entire device from the gamma knife using the adversary threat defined above. Select an insider from the 4 categories, considering how the insider will be assist the scenario (minimize adversary detection, minimize scenario delay and task time, facilitate access control, perform malicious act (sabotage device), or minimize response effectiveness.
C. Estimate the adversary delay along the scenario path, and the points of possible detection, along with their likelihood (H, M, L) using data generated in Exercises 3, 4 & 5. List equipment needed by adversary, along with weight. Estimate difficulty of tasks.
D. Employing response assumptions, estimate likelihood of security system effectiveness (i.e. estimate detection effectiveness and neutralization effectiveness) for the scenario.
E. Develop detection, assessment, access control, delay and/or response improvements to improve effectiveness
    a. Address core weakness(es) that was exploited by adversary (e.g. lack of detection, no assessment, lack of delay, weak access control, slow response…)
    b. Consider improvements to decrease effectiveness of insider
    c. Try to minimize cost of improvements
    d. Try to minimize operational impact of improvements
    e. Estimate detection and neutralization effectiveness and compare to requirement.

Output

Prepare a summary briefing of both scenarios, including results of all 5 steps for each scenario. Briefing should describe:

- type of insider selected, why this insider was preferred, and how insider was recruited;
- adversary scenario, including path;
- interruption and neutralization effectiveness
- core weakness exploited by adversary
- upgrades proposed, including costs and why they addressed core weakness(es)
- interruption and neutralization effectiveness after upgrade

Briefing does not require a slide presentation.

Scenario 2 Data

Insider selected and why: _____

_____

Target Facility and why: _____

_____

GLOBAL THREAT REDUCTION INITIATIVE

Adversary Scenario: Time of attack: _____

Adversary Equipment: _____

Steps/Path of Attack/Description/detection estimate/delay time:

1: _____

2: _____

3: _____

4: _____

5: _____

6: _____

7: _____

8: _____

9: _____

10: _____

Estimated Security Timely Detection Likelihood: _____

Estimated Neutralization Likelihood: _____

What is core weakness of security system against this scenario?

Detection: _____

Delay: _____

Response: _____

Planned Upgrades: _____

_____

_____

Upgraded Security Timely Detection Likelihood: _____

Upgraded Neutralization Likelihood: _____