SAND2008-6277C

Best Practices for Building Security Risk Assessment and Management

Rudolph V. Matalucci, Phd
for
Betty E. Biringer
Sharon L. O'Connor

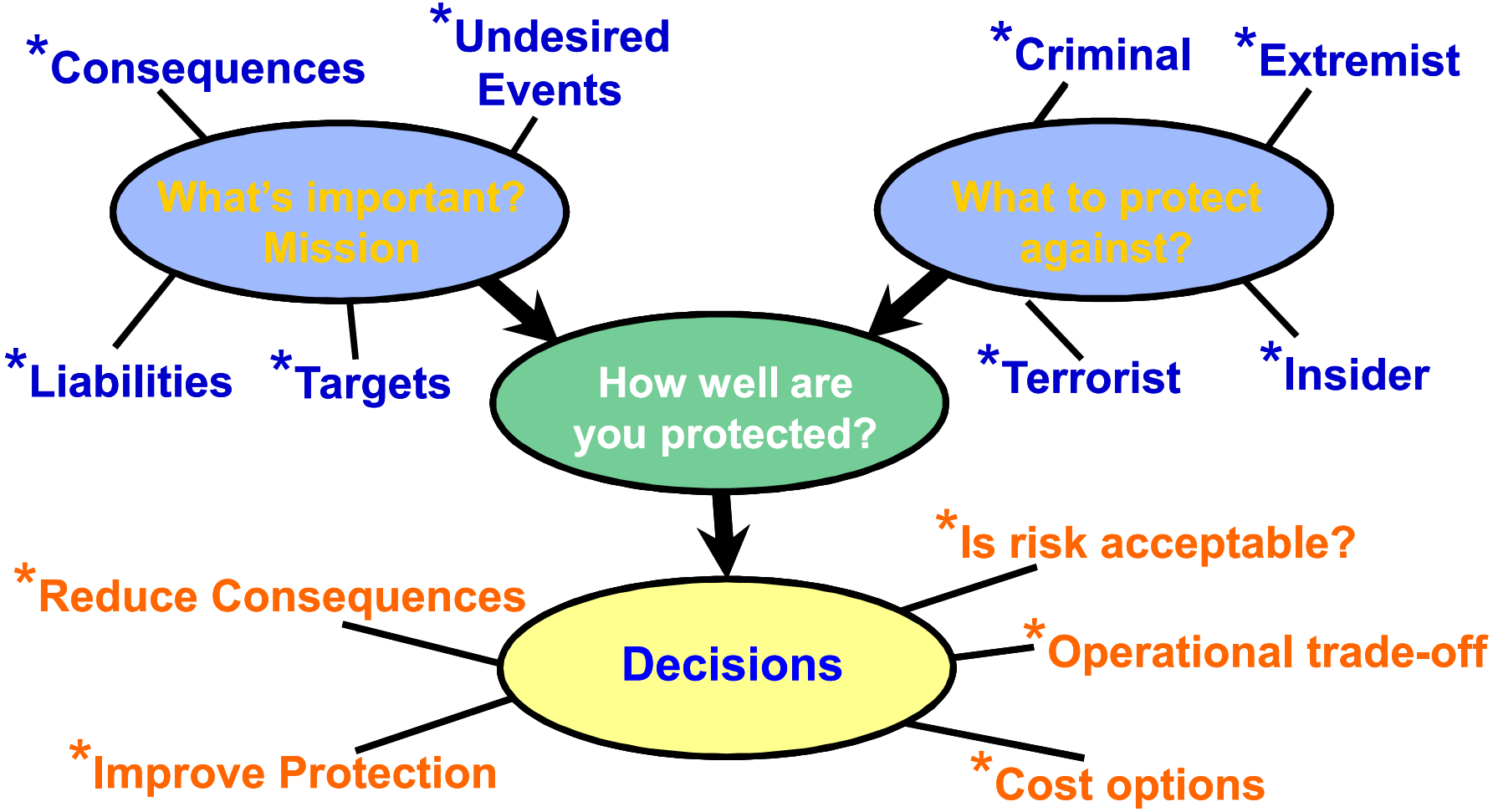
Sandia National Laboratories
Albuquerque, New Mexico 87185

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Sandia National Laboratories

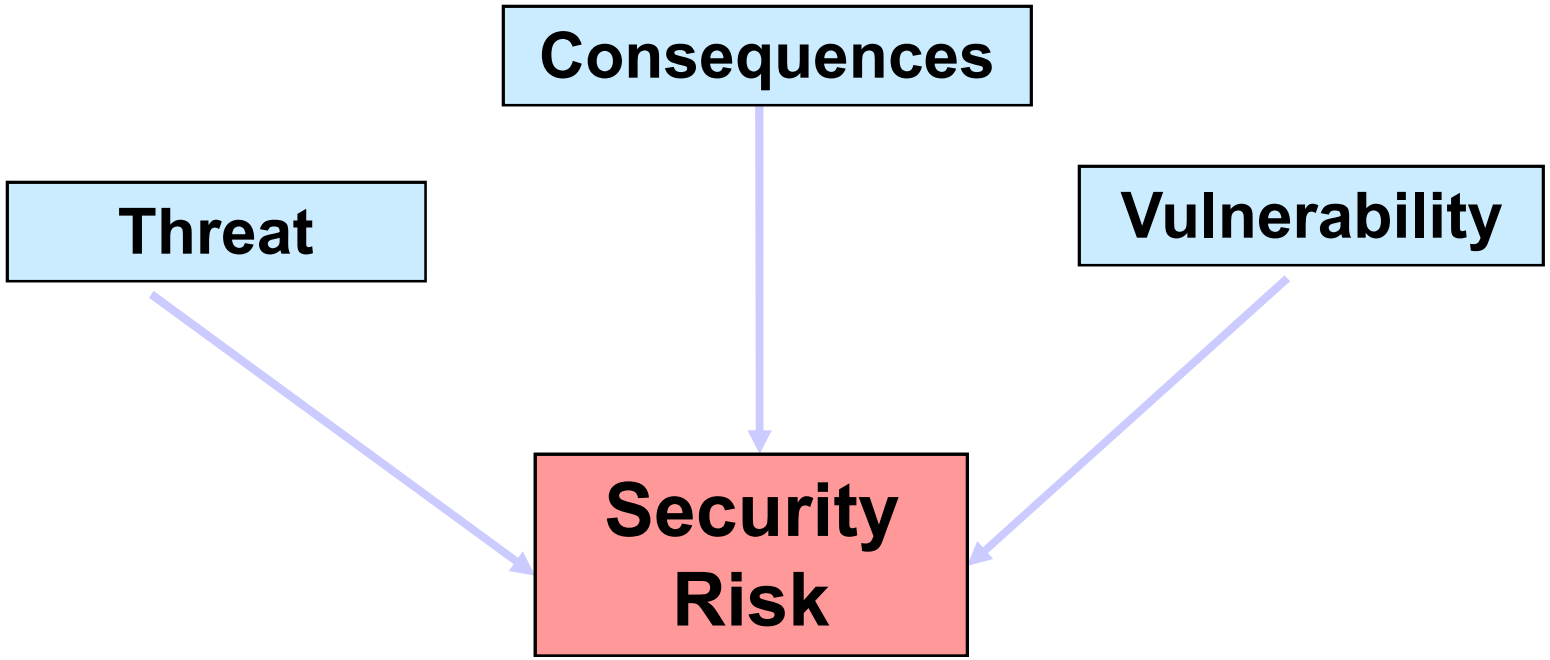
Sandia National Laboratories

How Much Security Is Enough?

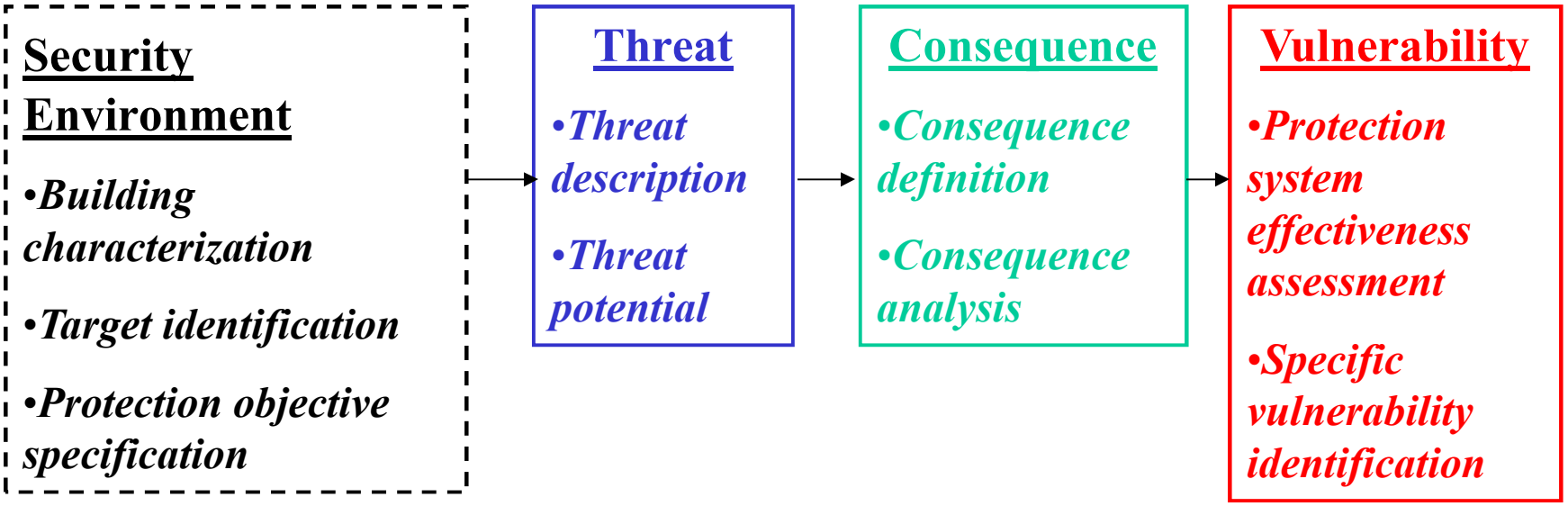


Sandia National Laboratories

Security Risk is a Function of:



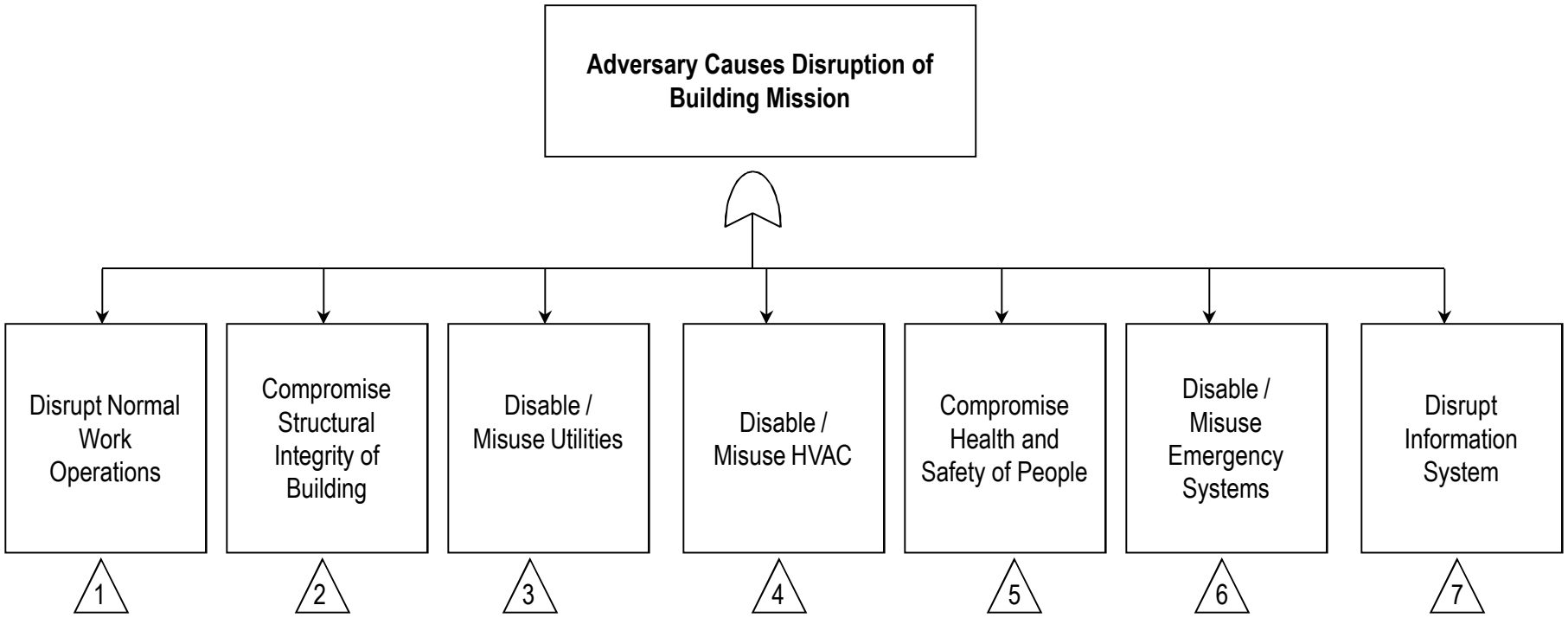
Security Risk Assessment



Building Characterization

- Building description
  - Physical layout and description
  - Information system architecture (process control/SCADA)
  - Mission/Operations
  - Physical and cyber protection system features
  - Work force
- Undesired events - what events to prevent
- Targets – what items to protect
  - Fault tree for building mission
- Protection objectives – prevent events or mitigate consequences

Top Events for Building Mission Fault Tree



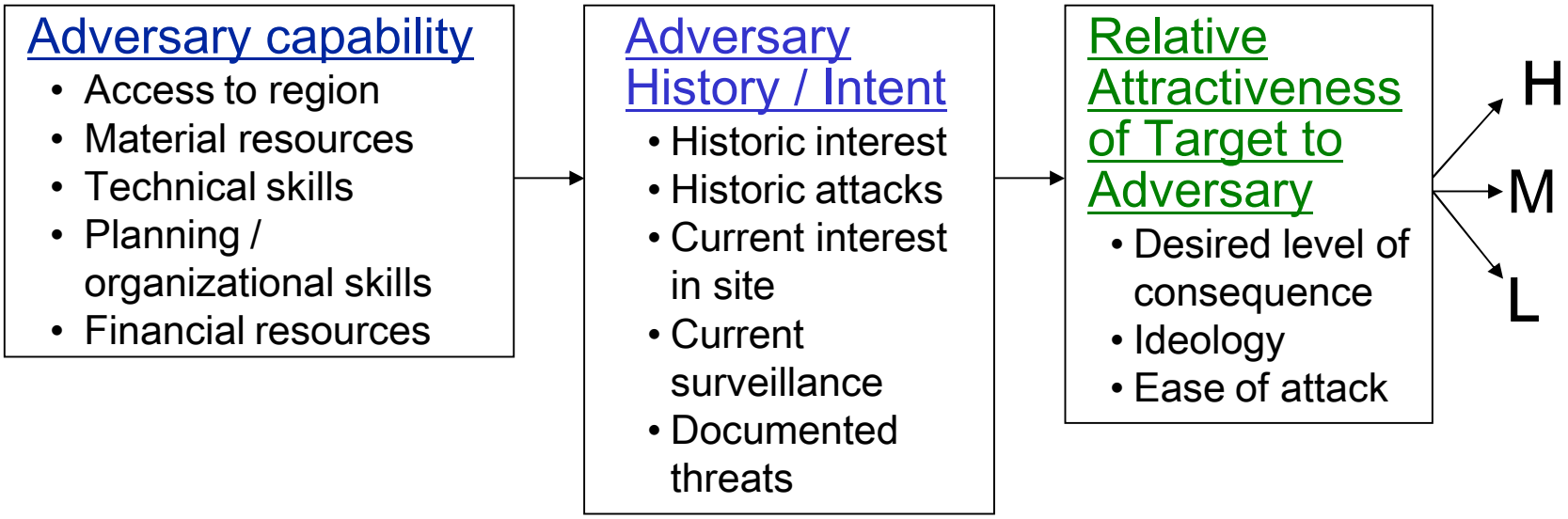
Sandia National Laboratories

Threat Definition

- Type of adversary
  - *Terrorists, criminals, extremists, militia, insider*
- Potential actions
  - *Theft, bombing, sabotage, damage*
- Motivations
  - *Ideological, economic, personal*
- Capabilities
  - *Numbers, weapons, equipment, transportation, technical experience*

Threat Potential

- Relative score – not a probability
- Scored per undesired event and per adversary group



Consequence Assessment

- Consequence of loss of the target should be developed.
- Establish units of consequence
  - Loss of human life
  - Loss of dollars
  - Loss of asset
  - Loss of operations/activity

- Rank in order of importance/value
- Assign relative value to each consequence

Sandia National Laboratories

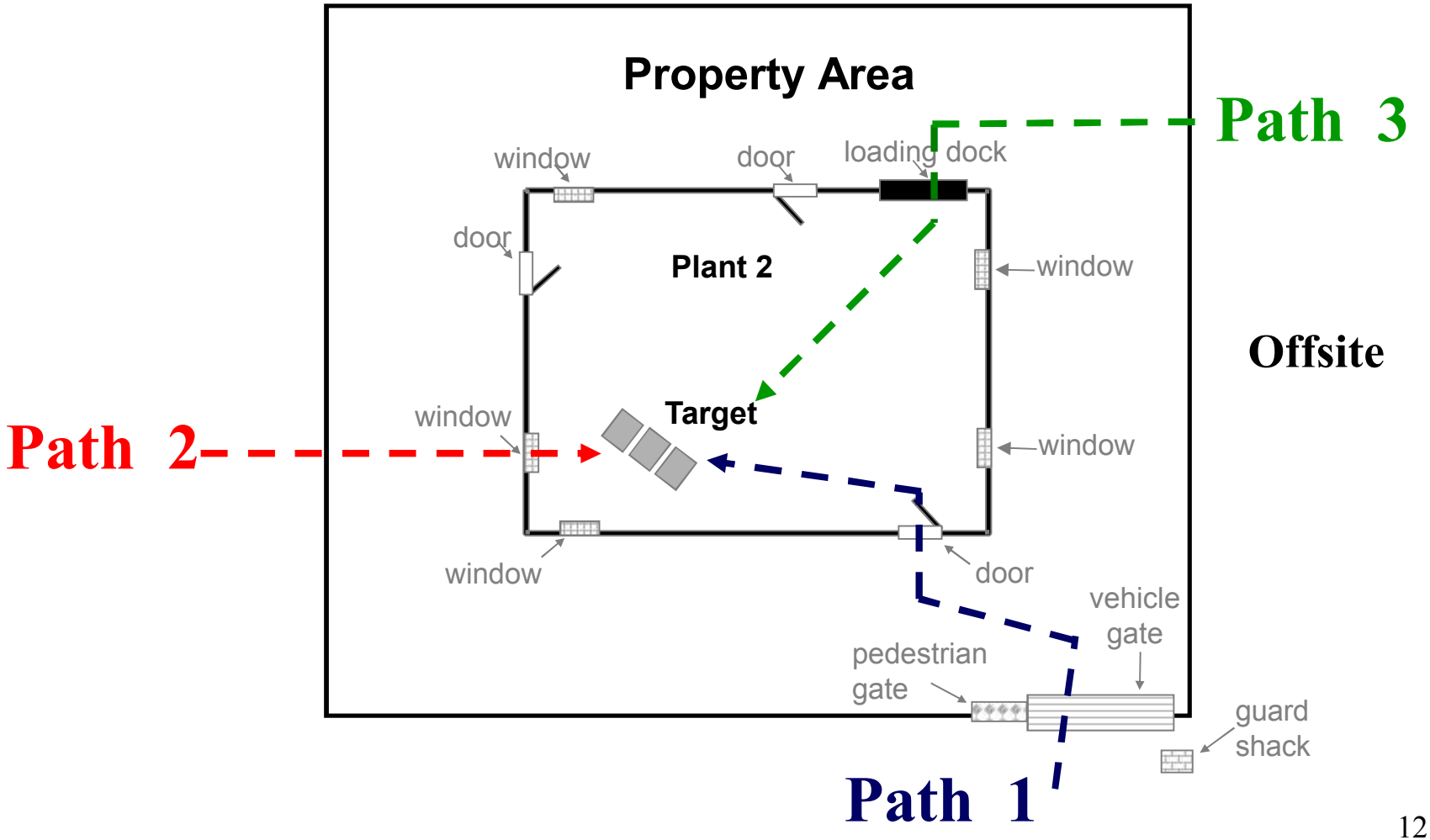
Sample Consequence Table

Measure of Consequence	High	Medium	Low
Economic loss (property loss + revenue)	> $5M	$1 – 5M	< $1M
Economic loss (users)	> $5M	$1 – 5M	< $1M
Deaths	>3	1 - 3	0
Geographic Impact	National	Regional	Local

System Effectiveness

- A measure of how effectively security system meets protection objective(s):
  - Physical attack: Prevent undesired event(s) with functions of detection, delay, response
  - Cyber attack: Preserve confidentiality, integrity, and availability of critical data with functions of authentication, authorization, audit

Physical Paths



Physical Protection Functions

Detection

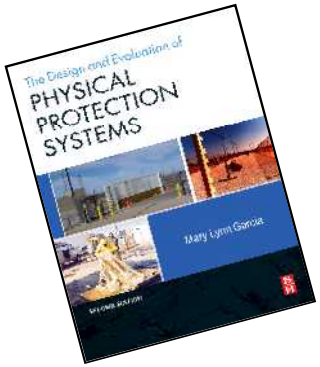
- Intrusion Sensing
- Alarm Communication
- Alarm Assessment
- Access Control
- Contraband Detection

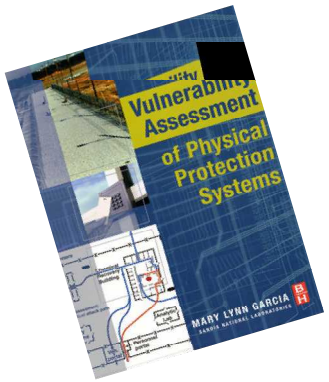
Delay

- Barriers
- Dispensable Barriers

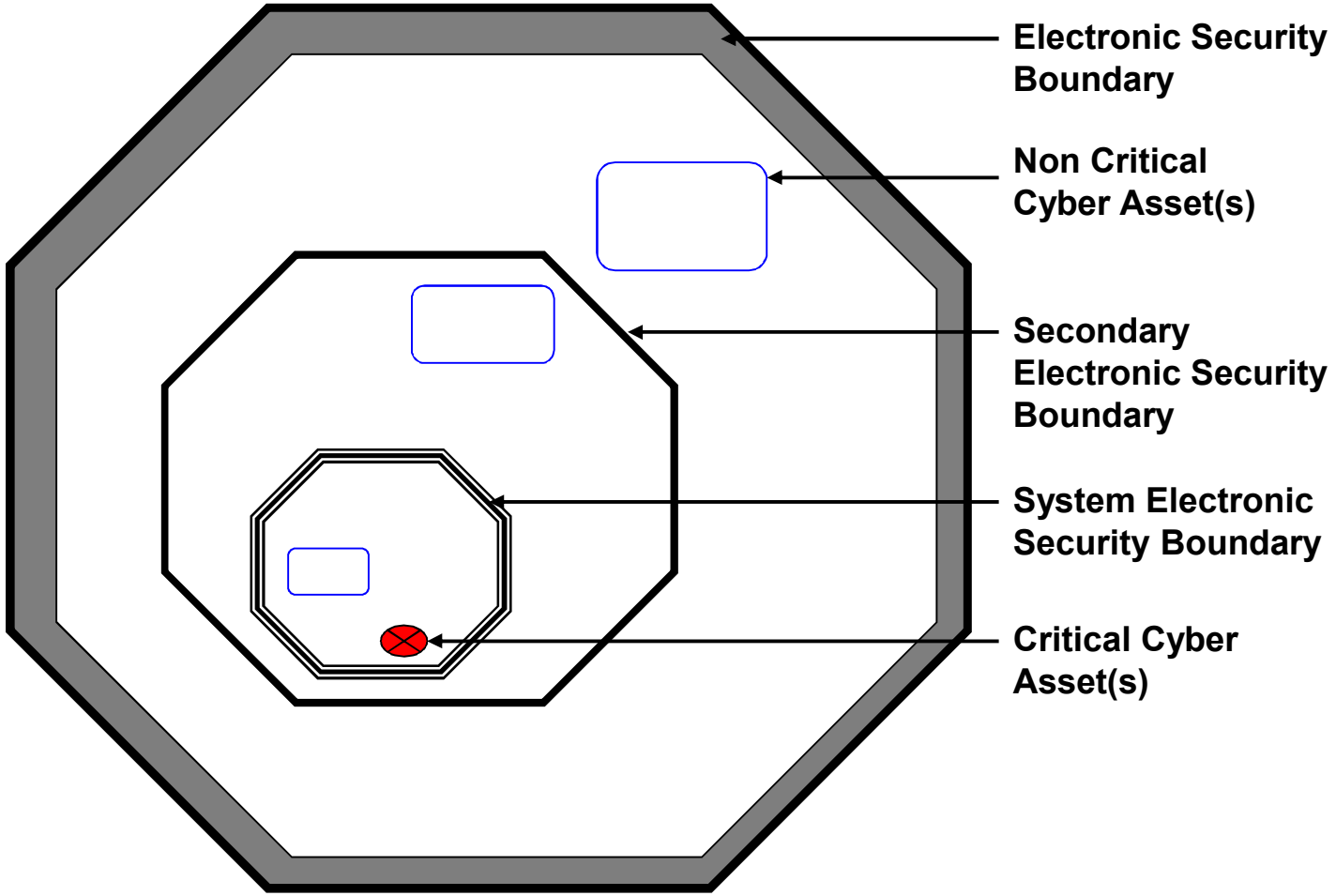
Response

- Interruption:
  - Communication to Response Force
  - Deployment of Response Force
- Neutralization





Cyber Paths


Electronic Security Boundary
Non Critical Cyber Asset(s)
Secondary Electronic Security Boundary
System Electronic Security Boundary
Critical Cyber Asset(s)

Sandia National Laboratories

Cyber Protection Functions

Authentication

- Validity of identity;

  Something you know

  Something you have

  Something you are

Authorization

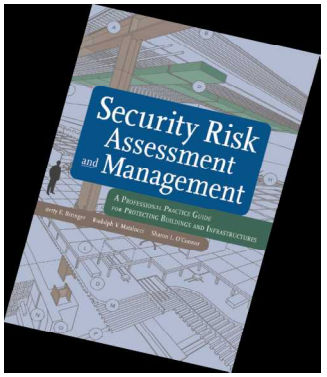
- Control access to information, systems, and applications
- Only authorized users can access assets based on authenticated identity

Audit

- Record actions or attempted actions
- Intrusion detection system

Sandia National Laboratories

Security Risk Assessment



Security Environment Description

Threat Assessment

Consequence Assessment

Vulnerability Assessment

Risk Estimation

Risk Acceptable?

Y

End (Periodic Review)

N

Propose Upgrades and Recommendations

Reducing Security Risk

- Reduce Threat level
  - Deterrence
  - Difficult to measure
- Reduce Vulnerability
  - Detection, Delay, Response
  - Authentication, Authorization, Audit
- Reduce Consequence level
  - Mitigation features
    - Redundant equipment
    - Function transfer
    - Structural hardening
  - Improve emergency response

Summary

- Security risk assessment provides valuable information for risk managers
  - Total system approach
  - Metrics
  - Addresses physical and cyber attacks
  - Defendable results: repeatable & traceable to original assumptions

- Method has been applied to buildings, dams, electric power transmission, chemical facilities, energy infrastructure, municipal water systems, prisons, & communities

Contact Information

Betty Biringer

Manager, Security Risk Assessment Department

(505) 844-3985

bebirin@sandia.gov

PO Box 5800, MS 0759

Albuquerque, NM 87185