



Risk Assessment for Biosecurity



International Biological Threat Reduction
Global Security Center
Sandia National Laboratories
April 2009

BEP-ANBio Workshop

SAND No. 2008-0480P

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





What Is “RISK”?

Risk can be thought of as taking a chance:

- Crossing a busy street
- Gambling in a casino
- Working with dangerous pathogens



Risk is a function of two variables:

- 1) The likelihood or the potential that an ***adverse event*** will occur
- 2) The associated ***consequences***





What is a Risk Assessment and Why Conduct One?

A risk assessment is a decision-making tool used for analyzing a complex process to:

- Determine which risks are acceptable and which are not
- Ensure that protection and the cost is proportional to the risk
- Determine where training should be focused
- Determine if certain activities or procedures should be modified
- Determine where valuable resources should be allocated
- Justify budget requests

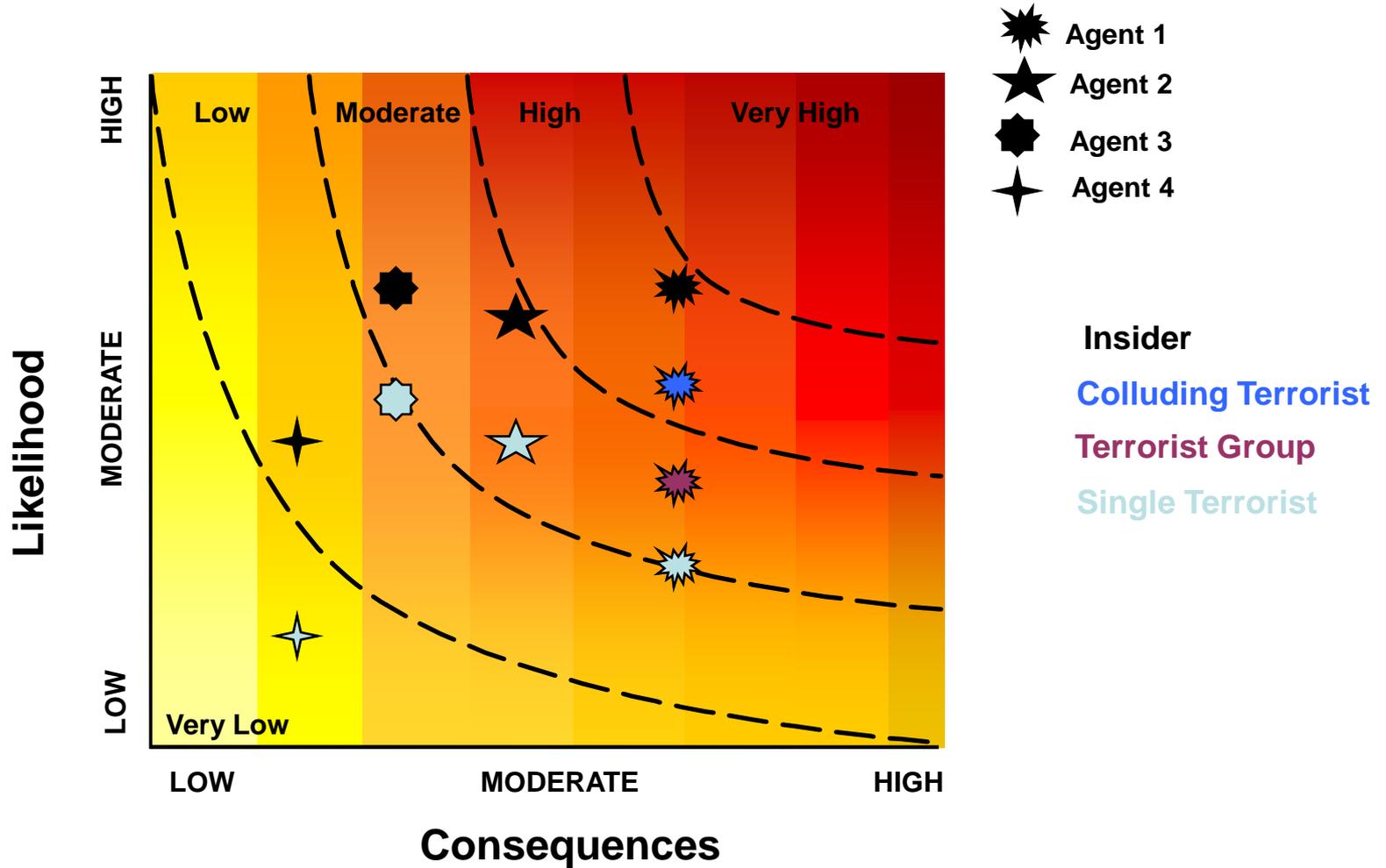


Biosafety R.A. vs Biosecurity R.A.

- **Biosafety is a series of measures implemented to protect people from dangerous biological agents**
 - A biosafety risk assessment analyzes the likelihood of someone *accidentally* becoming infected with a biological agent, and the resulting consequences
- **Biosecurity is a series of measures implemented to protect biological agents from dangerous people**
 - A biosecurity risk assessment analyzes the likelihood of a biological agent being *intentionally* used maliciously, and the resulting consequences



Output of Risk Assessment





Definitions

- 1. Asset – Something of value that should be protected. Example:**
 - a) A biological agent that could be used as a bioweapon
 - b) Anything of significant monetary value that could be stolen and sold
 - c) Something that if destroyed could jeopardize the success of the institution
 - d) Something of symbolic significance

- 2. Threat or Adversary – The person or group from which the asset is to be protected – The bad guy(s)**



4 Basic Steps of a Biosecurity Risk Assessment

1. Define the asset:

- What is valuable? Biological material, intellectual property, other property, etc
- The characteristics of the asset must be defined otherwise it would not be possible to determine the attractiveness to adversaries and consequences

2. Define the threat:

- The capabilities and resources of the threat must be defined otherwise it will not be possible to determine the potential of a successful attack.
- It is rarely possible to discriminate the potential consequences for a specific adversary so it is best to use the maximum credible consequences for all adversaries

3. Determine the worst-case consequences (x-axis of the graph)

4. Determine the likelihood of a successful attack by adversary (y-axis of graph)

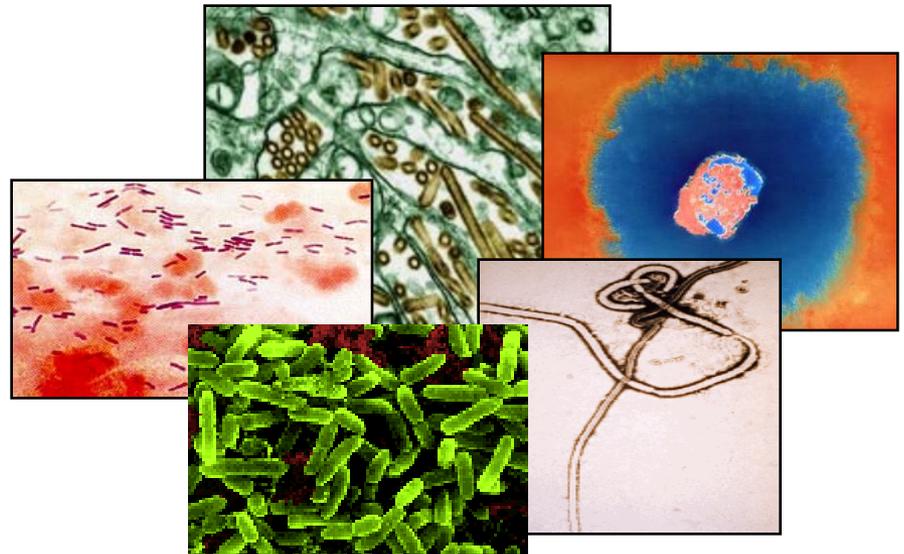


Step 1: Define the Asset

Assess the value of the agent from an adversary's perspective

For biological agents:

- Transmissibility
- Infection dose
- Morbidity
- Mortality
- Availability outside of lab
- Ease of storage
- Environmental stability
- Available treatment



For other assets:

- Monetary value
- Symbolic significance
- Value to institution beyond monetary, such as loss of productivity



Step 2: Define the Threat

Select a Threat Type

Select the type of threat:

Insider (Varying Degrees of Authorized Access)

Researcher with Authorized Access (Level 1)

Researcher with Authorized Access (Level 2)

Maintenance Worker

Management

Security System Administrator

Etc.

Outsider (No Authorized Access)

Criminal

Single Terrorist

Terrorist Group

Activist

Colluding Terrorist Group

Competitive Rival





Step 2: Define the Threat (Cont.)

Insiders vs. Outsiders

Scenarios involving Insiders generally pose a higher risk than scenarios involving Outsiders

Insiders

- Access to facility and buildings where biological agents are stored and used
- Can wait for an opportune time
- Have knowledge of facility operations and security system
- Some have relevant technical skills and know how to covertly remove the desired biological agent
- **Opportunity – yes**
- **Means – yes**
- **Motive – ?**

Outsiders

- Most biological agents can be readily found elsewhere
 - Other laboratories and in nature
- Do not have authorized access
- Have limited knowledge about facility operations and security
- Will not know exactly where the desired biological agent is stored
- Collusion with an Insider increases risk of detection
- **Opportunity – significantly less**
- **Means – typically less**
- **Motive – ?**



Step 2: Define the Threat

Example Notional Adversaries

Adversary 1 - Researcher with Authorized Access (Level 1):

- Ten researchers have authorized access to 500ml of the asset
- All are authorized to enter the laboratory at any time
- All have necessary expertise to grow the agent in a makeshift laboratory
- All are authorized to work in the laboratory alone
- Motive: Terrorism

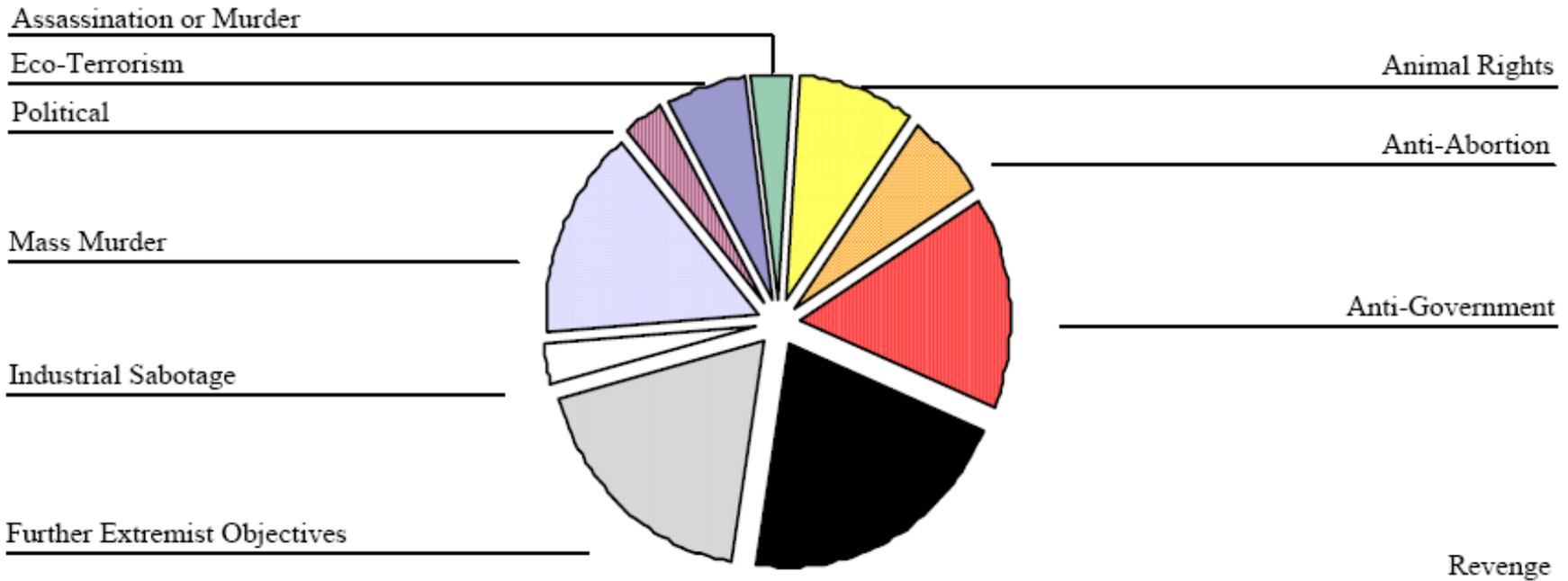
Adversary 2 – Criminal

- Assess capabilities by interviewing local law enforcement, site security, and intelligence community
- Assume this threat will use common hand tools, including battery operated power tools, to accomplish their tasks
- Assume a small group of two or three individuals working as a team
- Motive – Sell asset to extremist organization



Step 2: Define the Threat (Cont.) Bioterrorism and Biocrime Motives

- Review of 33 alleged incidents involving biological agents from 1960 to January 1999



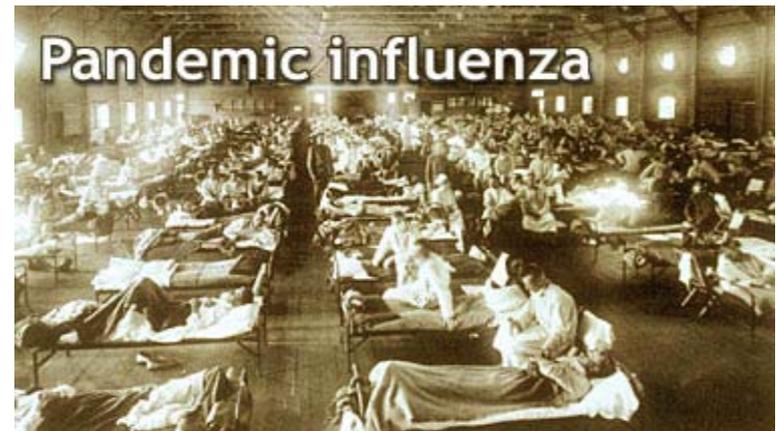
Reference: [Historical Trends Related to Bioterrorism: An Empirical Analysis](#)
by Jonathan B. Tucker, Monterey Institute of International Studies



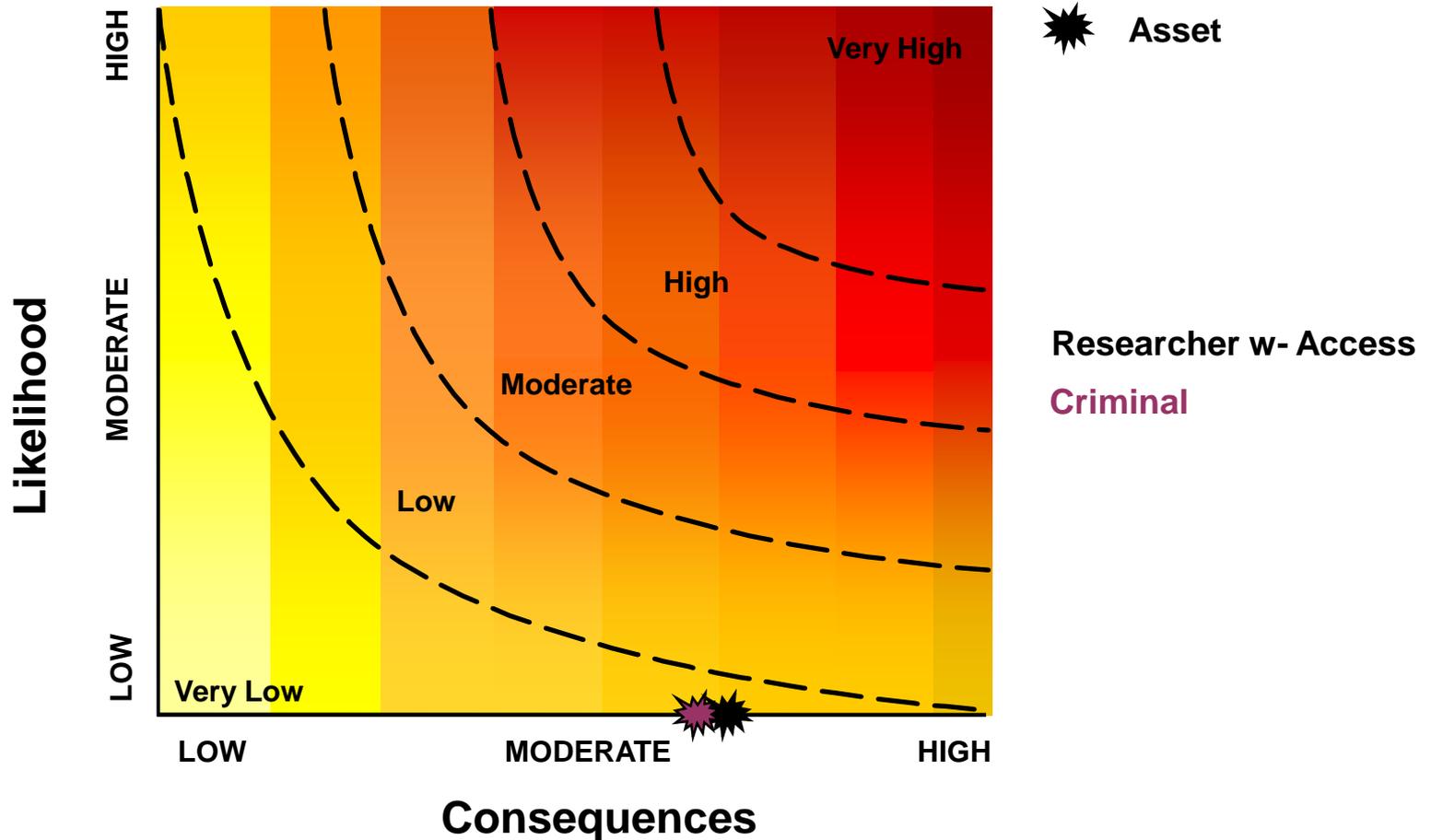


Step 3: Determine Worst Case Consequence

- Given the *asset definition* and the *threat definition*, determine the maximum credible consequences, consider:
 - Impact to population (mortality and morbidity)
 - Impact to economy
 - Psychological impact



Output of Risk Assessment (So Far)





Step 4: Determine Potential of Successful Attack

Sequence of a successful biological attack – applies to both insiders and outsiders

- a) Plan attack
- b) Acquire biological agent
- c) Transport biological agent to makeshift laboratory
- d) Grow the agent to obtain the desired quantity (unless a sufficient quantity is acquired)
- e) Prepare the agent for a suitable form for dissemination
- f) Manufacture dispersal device (depends on the biological agent)
- g) Transport biological agent to point of attack
- h) Disseminate biological agent



Step 4 – Determine Potential for Successful Attack

Example Scenario for Acquiring a Biological Agent (Insider)

Example Theft Scenario for Criminal Threat

1. Enter the lab on weekend – take lunchbox with ice pack
2. Enter lab using authorized credential
3. Remove agent from freezer and insert into ice pack of lunch box
4. Replace missing vial with dummy vial containing material that looks like original.
5. Take agent home and put in freezer



Step 4b – Evaluate Countermeasures

For each step in the scenario, evaluate effectiveness of existing countermeasures

Countermeasures:

1. Must have justification letter signed by supervisor for working in lab after hours
2. Limit which personnel have authorized access to only those working with biological agents
3. Personnel reliability program



Step 4 – Determine Potential for Successful Attack

Example Scenario for Acquiring a Biological Agent (Outsider)

Example Theft Scenario for Criminal Threat

1. Attack at night on a Saturday at approximately 3:00am
2. Wait for the patrolling guard to pass then cross the site perimeter at the north side of the campus
3. Proceed to Building xx
4. Enter Building xx through a window on the east side of the building where it is darkest. Look for open window before forcing entry.
5. Once inside the building, search for a laboratory where biological agent is kept (hoping to find signage on the door)
6. Force the door to the laboratory open with a pry bar
7. Force open refrigerator and freezer doors
8. Look for biological agent inside refrigerator/freezer (hoping for labels on containers)
9. Look for inventory sheets to help locate biological agent of interest
10. If unsuccessful in locating specific contain, fill backpack with as many containers as possible.
11. Exit the building and site using same path as entry
12. Try to sell the biological agents to an extremist group



Step 4b – Evaluate Countermeasures

For each step in the scenario, evaluate effectiveness of countermeasures

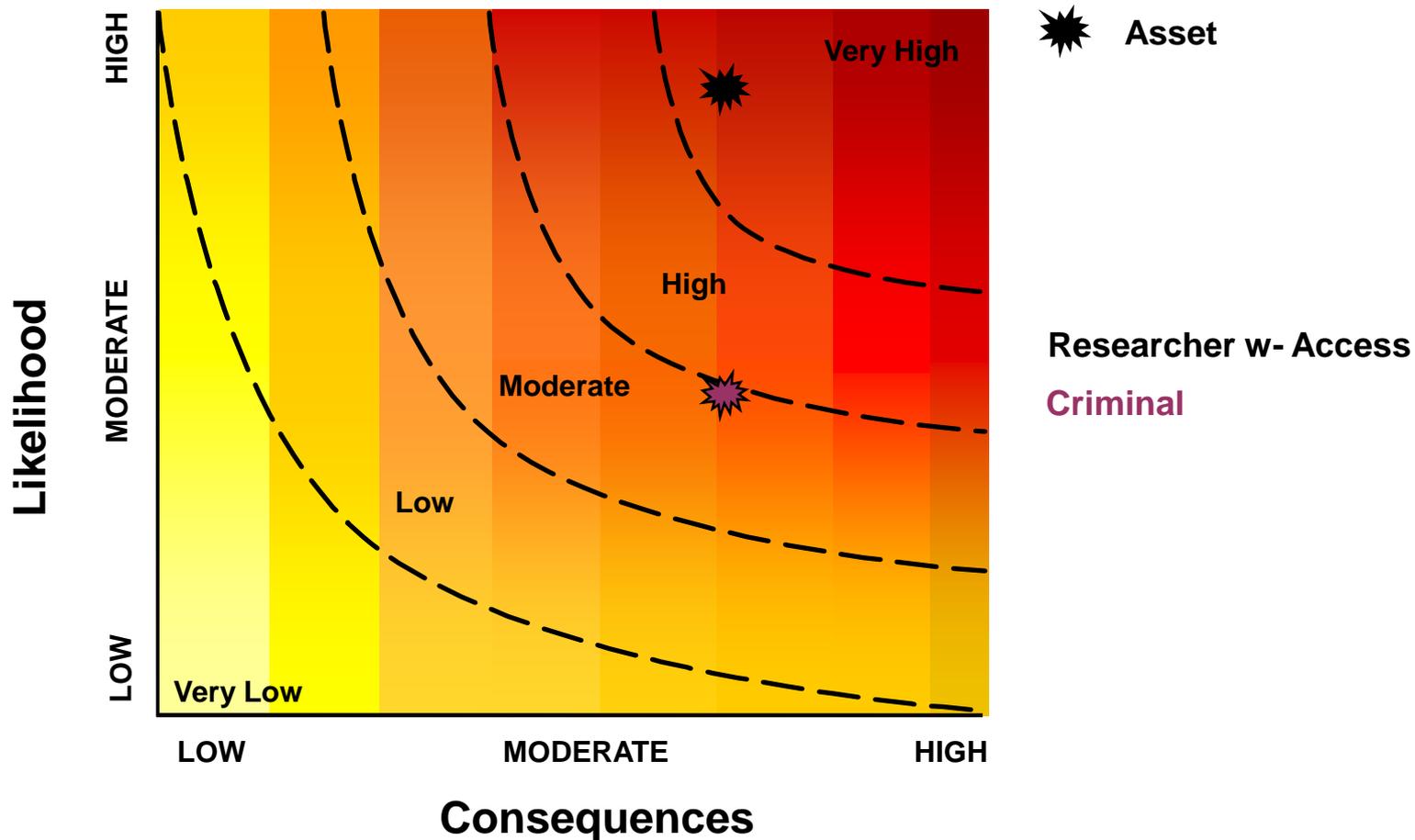
Example, step 4 in scenario: Enter Building xx through a window on the east side of the building where it is darkest. Look for open window before forcing entry.

Countermeasures:

1. Standard operating procedure is to close and lock all windows before leaving for the night.
2. Electronic access controls on doors which are alarmed if opened without authorization
3. All windows are equipped with position sensors and glass break sensors



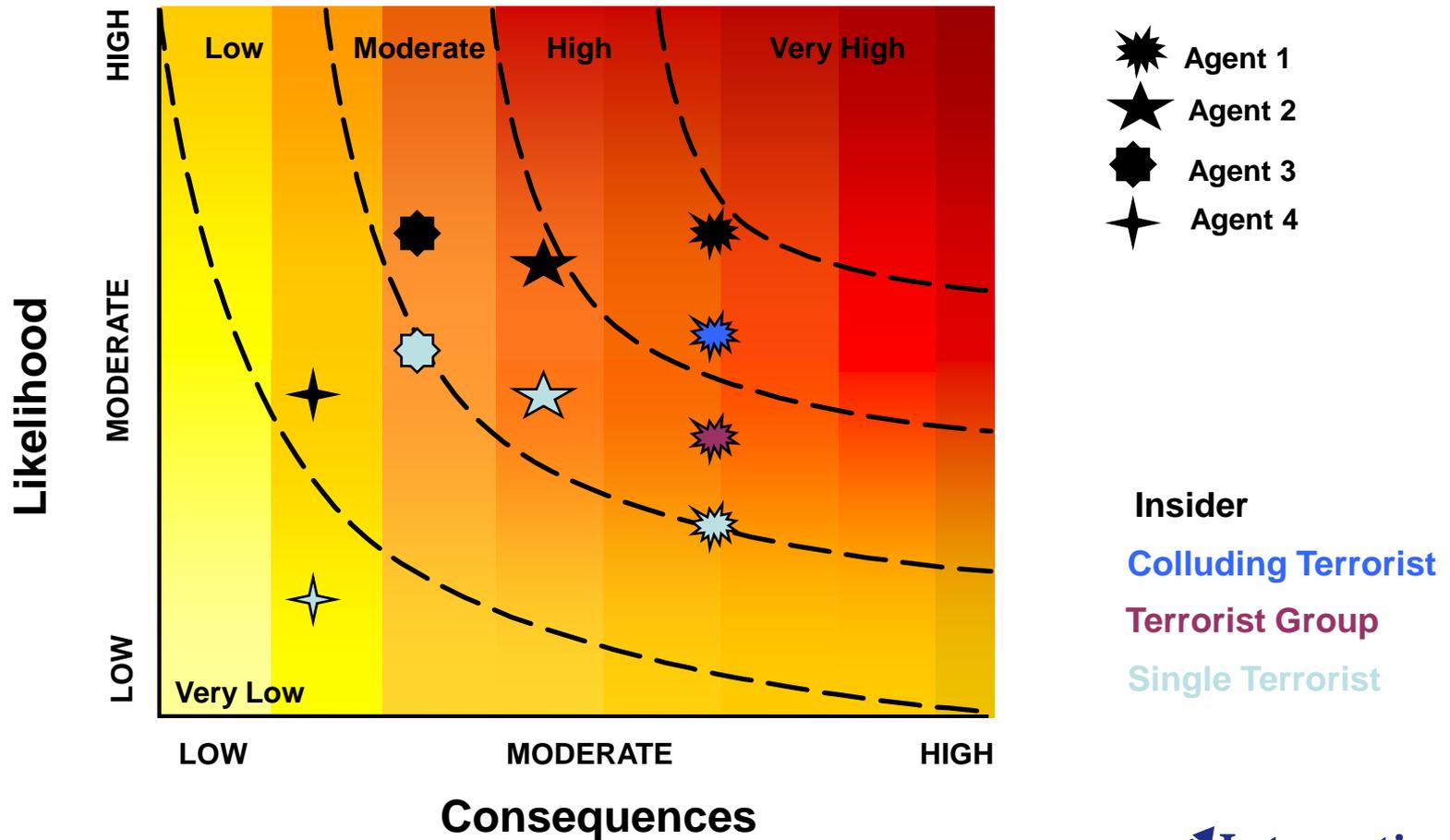
Hypothetical Results of Risk Assessment





Hypothetical Risk Results

Repeat the process for all asset/threat combinations





Risk Management Principles

1. **Determine which risks are acceptable and which are not**
2. **Make modifications to the facility, procedures, security force, etc., to reduce unacceptable risks to an acceptable level**
3. **Develop incident response plans for acceptable risks**

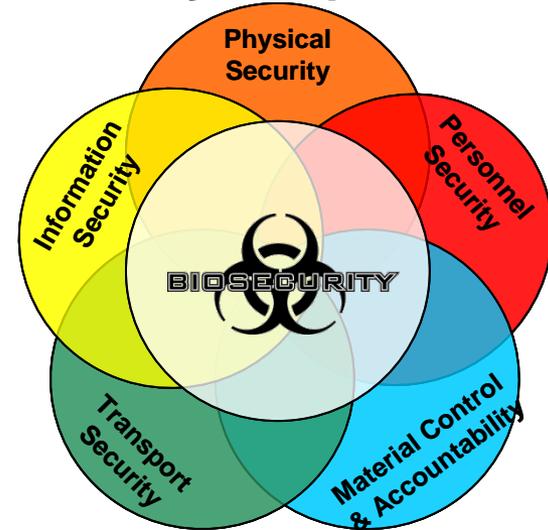
REMEMBER:

- a) Risk can never be totally eliminated. It is not possible to protect every asset from every conceivable threat.
- b) A graded approach should be taken when applying protection strategies
- c) The level of risk reduction that can be achieved is exponentially proportional to cost



Biosecurity Risk Management

- **Evaluate the effectiveness of each current biosecurity component of the existing laboratory system**
 - Physical security
 - Personnel security
 - Material handling and control measures
 - Transport security
 - Information security
 - Program management practices
- **Example: physical security vulnerability assessment**
 - Are access controls in place at buildings and laboratories where the biological agents are stored and used?
 - Also consider:
 - **Intrusion detection systems**
 - **Site perimeter**
 - **Response force**



RISK
PERCEPTION

RISK
ASSESSMENT

RISK
MANAGEMENT

