



Biosecurity Risk Assessment

Biosecurity Inspector Training

**Staten Serums Institut
31 August – 2 September 2009**

www.biosecurity.sandia.gov

SAND No. 2009-5485C

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.





Risk Definitions

- **Risk Assessment**
 - Identifying and exploring, preferably in quantified terms, the types, intensities and likelihood of the consequences related to a risk. Risk assessment comprises hazard identification and estimation, exposure and vulnerability assessment and risk estimation
- **Risk Analysis**
 - Risk assessment, risk management, and risk communication
- **Risk Prevention**
 - Measures to stop a risk being realized; typically means stopping the activity giving rise to the risk
- **Risk Reduction**
 - Measures to reduce the level of risk, for example by reducing the likelihood of the risk being realized or reducing the impact of the risk



Risk Assessment

- **Purpose:** understand uncertain but possible consequences associated with specific hazards
- **Components:**
 - Hazard identification and estimation
 - Assessment of exposure and/or vulnerability
 - Estimate of risk based on hazards and exposure/vulnerability assessment
 - **Combining likelihood and severity of selected consequences**
 - **Quantitative or qualitative**
- **Discussion: Current risk assessment methods used for biorisks**
 - How are hazards identified and estimated?
 - How are exposures and vulnerabilities assessed?
 - How are the likelihood and severity of consequences determined?



Risk Assessment Process

- **A standardized biological risk assessment process allows the risk assessments to be:**
 - Repeatable
 - Quantifiable
- **A systematic, standardized approach should include:**
 - Accepted criteria for assessing the risk
 - A standardized approach for evaluating the situation against the criteria (“scoring system”)
- **Ideally this process results in a system that:**
 - Allows analysis of the risk to identify driving factors and allow better realization of mitigation measures
 - Enables better communication of risk
 - **Help to define what is acceptable risk**





Risk = f (Likelihood, Consequence)





Laboratory Biosecurity Risks for Dangerous Pathogens

$$\text{Risk} = f(\text{Likelihood, Consequence})$$

- **Likelihood**
 - The likelihood of theft from a facility and the likelihood an agent can be used as a weapon
- **Consequences**
 - Of a bioattack with the agent
- **Risks**
 - Persons in area of attack
 - Persons in larger community from secondary exposure
 - Animals in area of attack
 - Animal in larger community from secondary exposure



Biosecurity Risk Assessment

- 1. Characterize biological agents and threats**
 - a. Evaluate pathogens and toxins at a facility (Asset Assessment)
 - b. Evaluate adversaries who might attempt to steal those pathogens or toxins (Threat Assessment)

- 2. Characterize the facility**
 - a. Evaluate the likelihood the facility will be targeted
 - b. Evaluate the likelihood of a successful theft (Vulnerability Assessment)

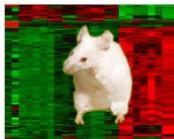
- 3. Characterize the risk**
 - a. Evaluate the overall likelihood and consequences of each scenario
 - b. Determine acceptable and unacceptable risks; develop risk statement





Evaluation of the Pathogens and Toxins

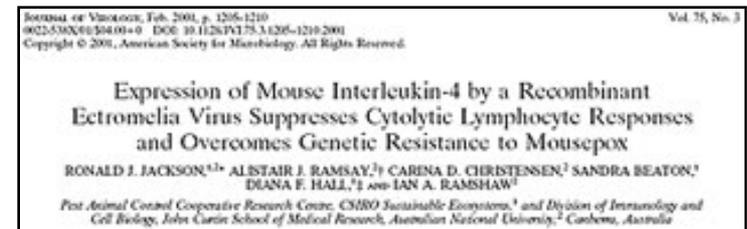
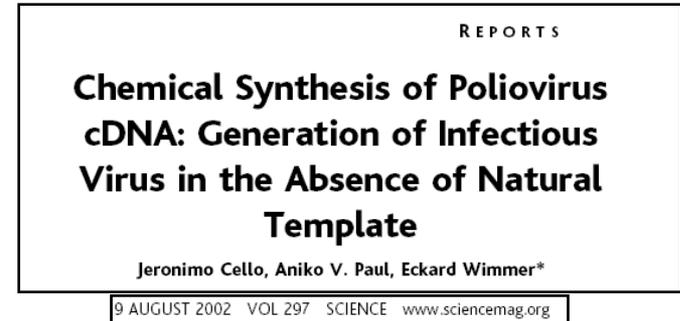
- **Not all biological agents have the same risk**
- **Identification of a 'target' is difficult for biological agents/materials**
 - Microbes cannot be counted
 - The 'target' or asset may be all over a room, inside an animal, in the waste system, etc
 - Microbes cannot necessarily be detected if missing (an entire tube may be detected but not a microbe from within)





Characterize the Biological Agents

- Agents potential as a biological weapon
 - **Biological Agent Properties**
 - Transmissibility
 - Stability
 - Awareness of agent's BW potential
 - **Production and dissemination**
- Consequences of a bioattack with agent
 - **Disease consequences**
 - **Socioeconomic consequences**
 - **Secondary exposure consequences**





Other Assets at Biological Facilities

- **Security Information or Systems**
 - May be targeted to facilitate access to dangerous biological materials
- **Other Facility Assets**
 - May be targeted by political extremists, disgruntled employees, etc.
 - May include:
 - **High containment laboratories**
 - **Animals**





Characterize the Adversaries

- **Adversary Classes**

- Should be defined in design basis threat
 - Terrorist
 - Extremist
 - Criminal



- **Insiders**

- Authorized access to the facility, dangerous pathogens, and/or restricted information
- Distinguish Insiders by level of authorized access
 - Site
 - Building
 - Asset



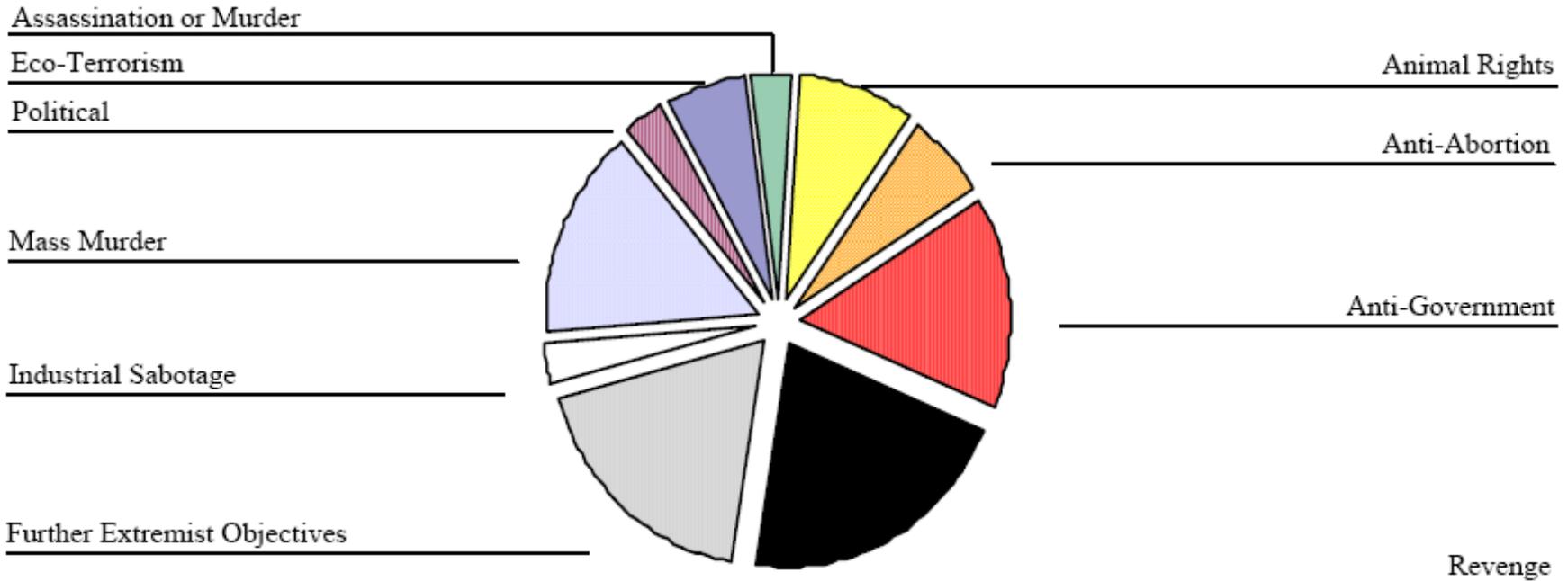
- **Outsiders**

- No authorized access



Bioterrorism and Biocrime Motives

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





Evaluate the Potential Adversaries

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 – ?**



Characterize the Facility

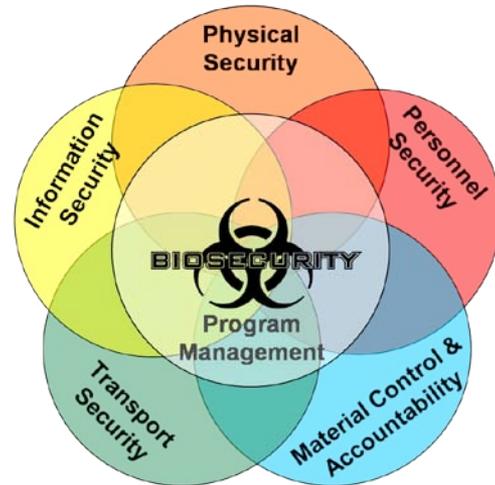
- **Identify “specific adversaries”**
 - Operational Means
 - Opportunity

- **Identify “specific assets”**
 - Uniqueness of asset at facility
 - Location of asset
 - State of asset (e.g. in long-term storage, in active research, type of research, quantity, ...)



Facility Vulnerability Assessment

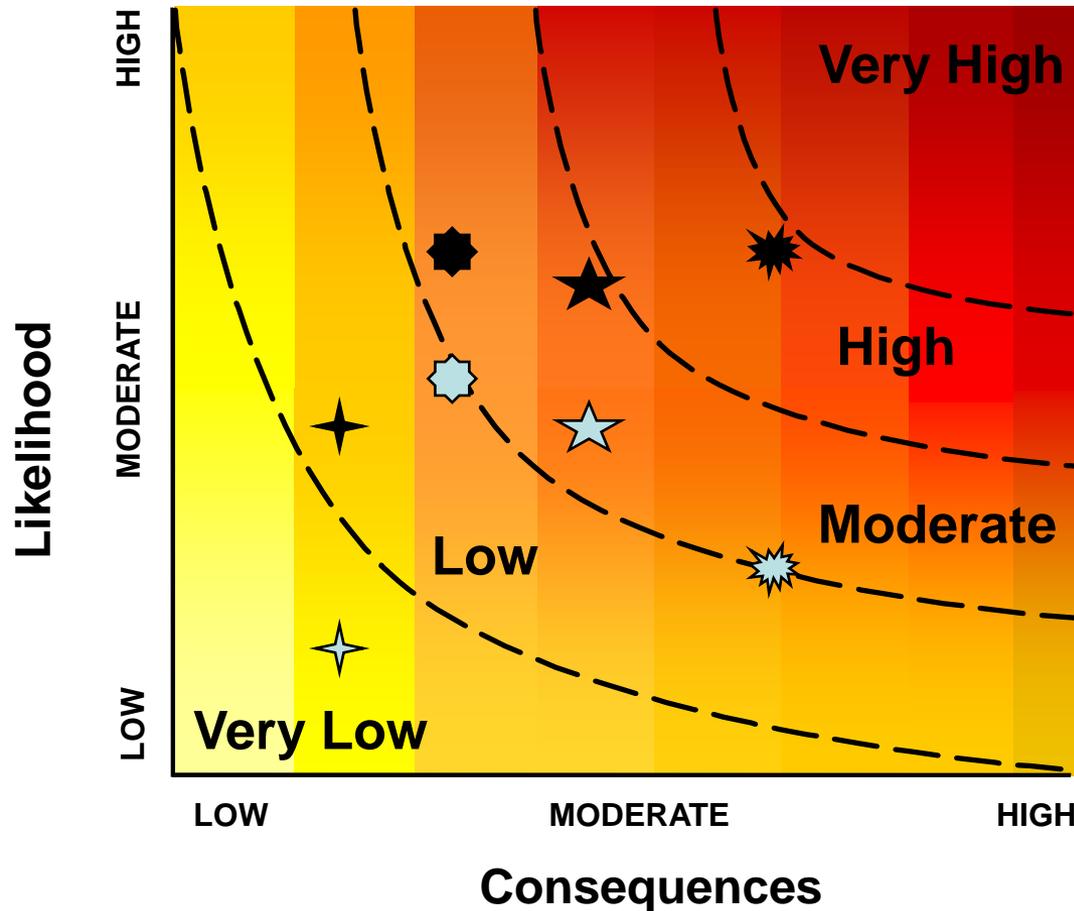
- **Identify mechanisms each defined adversary could achieve their objective**
- **Identify vulnerabilities in the biosecurity system**
 - Physical security
 - Personnel security
 - Material handling and control measures
 - Transport security
 - Information security
 - Program management practices





Characterize the Risk

- Who decides what is acceptable, tolerable, and intolerable?



● Protect against intolerable risk scenarios

● Develop incident response plans for acceptable risk scenarios