
Risk Assessment as a Foundation for Laboratory Biosecurity

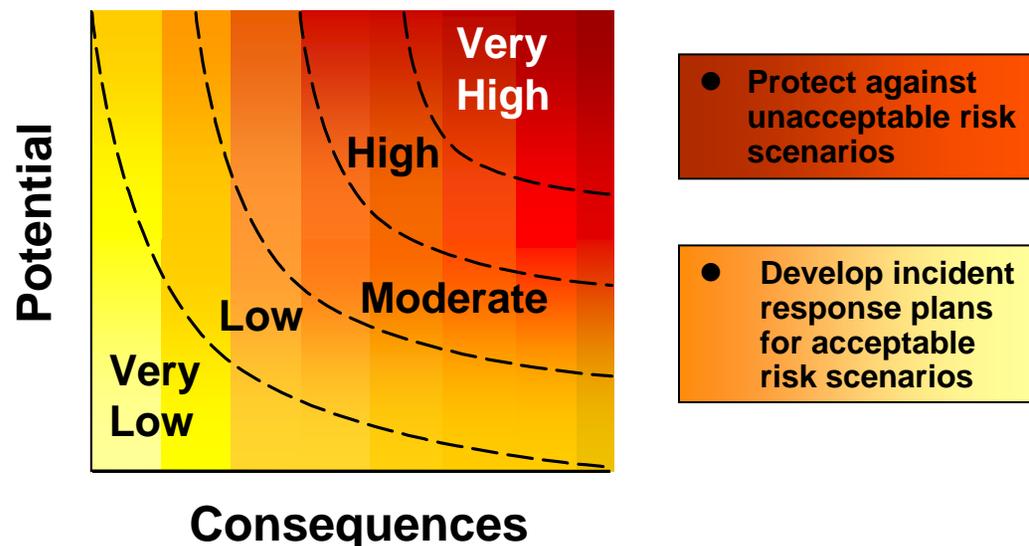
**International Biological Threat Reduction Department
Sandia National Laboratories
October 07, 2007**

**Managing a Laboratory Biosecurity Program
ABSA pre-conference course**

Biosecurity Based on Risk Management



- Is a function of the likelihood an adverse event will occur
 - $\text{Biosecurity Risk} = \text{Threat Potential} * \text{Consequences}$
- Cannot eliminate risk
 - Management must determine which risks are unacceptable (risk decision)
- Risk assessment is key to resource allocation
 - Graded protection
 - Existing resources should be used efficiently
 - Ensure that protection and the cost is proportional to the risk



Laboratory Biosecurity

- **Biosecurity System**
 - **Not limited to theft and deliberate misuse of biological agents**
 - **Assessment based methodology**
 - **Can be applied to other important laboratory assets**
 - **Computers**
 - **Laboratory notebooks and notes**
 - **Can be applied to other malicious actions**
 - **Sabotage**
 - **Theft of other assets**

- **As a minimum, every laboratory biosecurity system should consider strategies to minimize the risk**
 - **Theft and deliberate misuse of dangerous biological agents**

Biosecurity Risk Assessment

- 1. Characterize assets (pathogens and toxins) and threats**
 - a. Evaluate pathogens and toxins at facility (asset assessment)**
 - b. Evaluate adversaries who might attempt to steal those pathogens or toxins (threat assessment)**

- 2. Evaluate scenarios**
 - a. Create scenarios consisting of specific adversary attempting to steal and misuse a specific biological agent**
 - b. Determine how the various scenarios could be perpetrated (vulnerability assessment)**

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



Asset Assessment

- **Assess value of the agents from an adversary's perspective**
 - **Consequences**
 - **Population**
 - Transmissibility
 - Mortality
 - Morbidity
 - **Economic**
 - **Psychological**
 - **Task Complexity**
 - **Acquisition**
 - Natural
 - Laboratory
 - Synthetic biology
 - **Production**
 - R&D
 - Covert production
 - Ease of storage
 - **Dissemination**
 - Route of infection (e.g. aerosol, ingestion)
 - Environmental hardiness



Assessment result:

Nonpathogenic

Malicious Use Risk:

Low, Moderate,
High, Extreme

Threat Assessment

- **Adversary Classes**
 - 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
 - Facility management, site security, and local law enforcement interviews
- **Outsiders**
 - No authorized access
 - Local law enforcement, site security, and intelligence community interviews



Evaluate Scenarios

- **Scenarios of specific adversaries attempting to steal and misuse specific pathogens or toxins**
 - **Can screen assets that do not present sufficient risk**
 - **Nonpathogenic and LMUR**
 - **Can screen adversaries for certain scenarios because they have no interest in biological agents or have insufficient means**

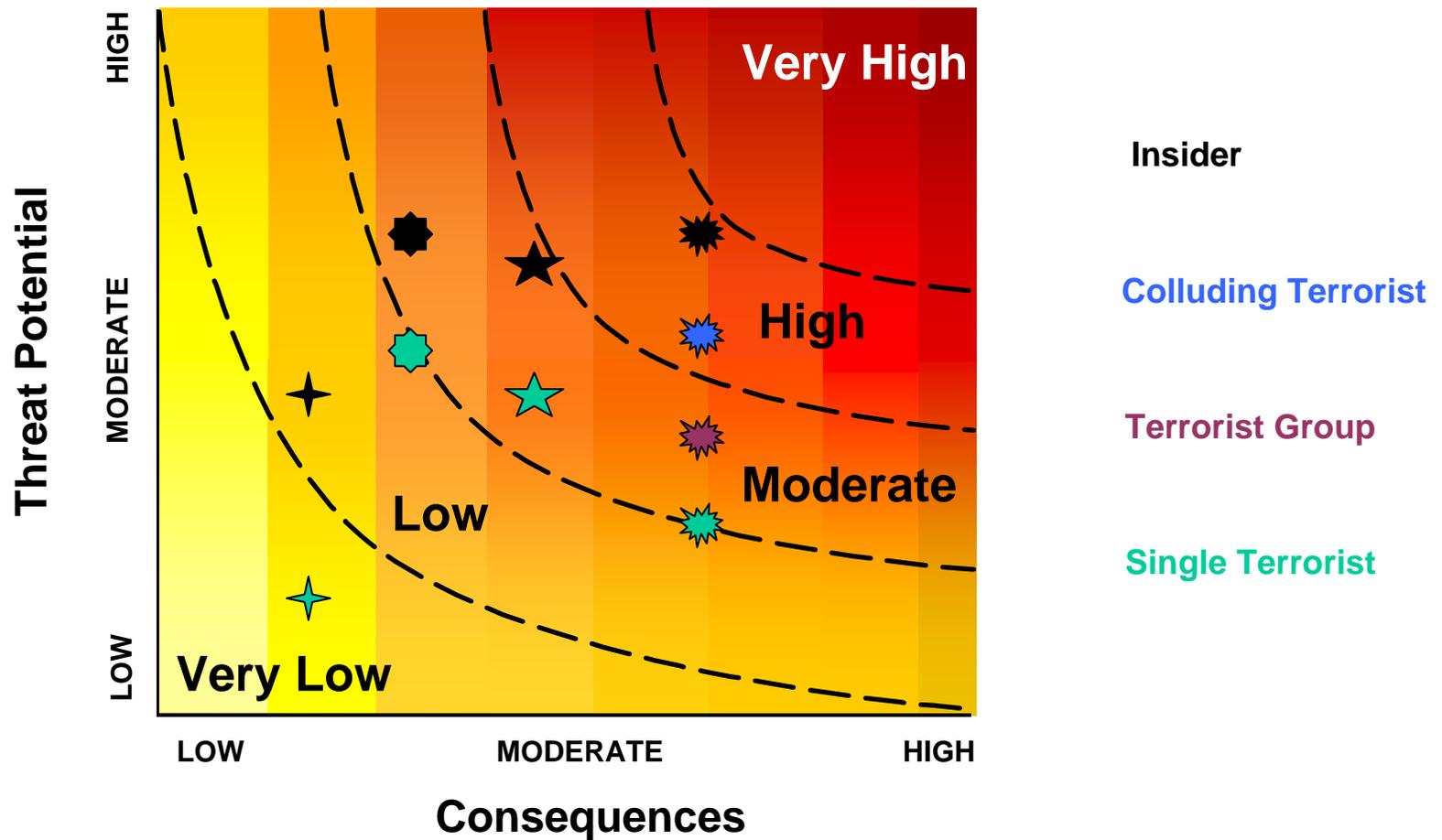
| Asset | Adversary | Action |
|-------|---------------------------|---------------------------|
| EMUR | Insider | Theft of biological agent |
| EMUR | Terrorist group | Theft of biological agent |
| EMUR | Colluding terrorist group | Theft of biological agent |
| HMUR | Insider | Theft of biological agent |
| HMUR | Terrorist group | Theft of biological agent |
| HMUR | Colluding terrorist group | Theft of biological agent |
| HMUR | Single terrorist | Theft of biological agent |
| MMUR | Insider | Theft of biological agent |
| MMUR | Single terrorist | Theft of biological agent |

Vulnerability Assessment

- Do vulnerabilities exist that allow defined scenarios to occur?
- For biosecurity risk assessment, evaluate existing laboratory biosecurity system
 - Physical security, Personnel security, Material control & accountability, Transport security, Information security, Program Management
- Physical security vulnerability assessment
 - Are access controls in place to buildings and laboratories where the biological agents in the scenarios are stored and used?
 - For scenarios with outsiders, evaluate
 - Intrusion detection systems
 - Site perimeter
 - Response force

Characterize the Biosecurity Risk

Hypothetical Risk Results



Conclusions

- **Not all pathogens and toxins warrant the same level of laboratory biosecurity**
- **Risk assessment is the fundamental resource allocation tool**
 - **For making decisions about which risks need to be protected against**
- **Risk assessment and risk decision are the critical foundation for the design of a physical security system**