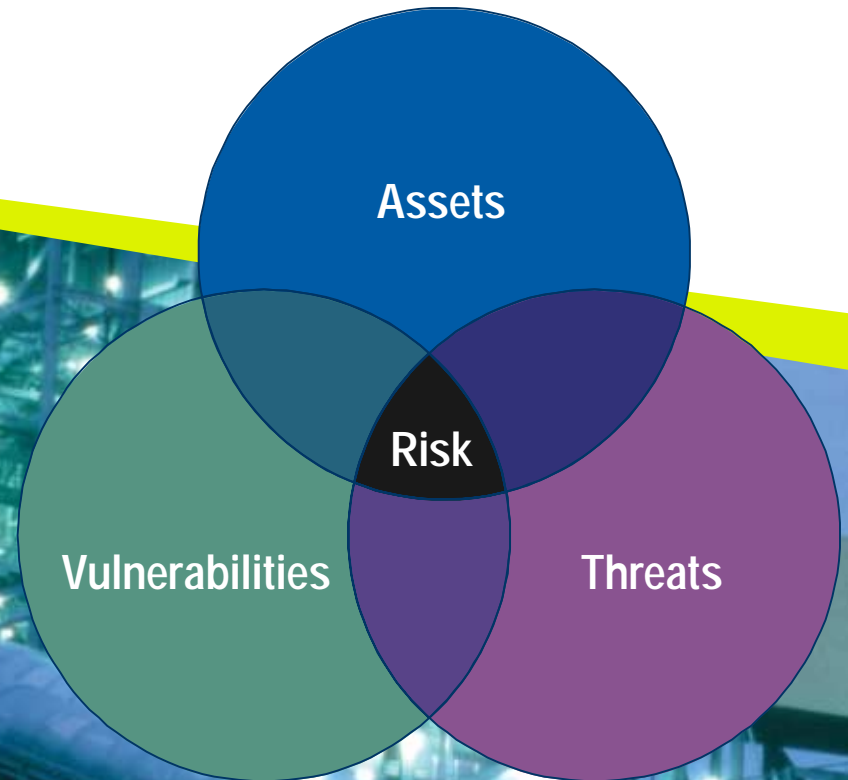




# Managing Risk in Today's Work Environment



# Combating Terrorism



- Measures and precautions need to be enforced across the operational continuum
- Focus on stopping a terrorist act before it happens; away from the installation
- Reduce vulnerabilities by providing conditions unfavorable to the terrorist
- Success is not having a loss of life, equipment, or material

# Terrorism, as Defined by the DOD



**Ter·ror·ism ('ter-ər-,i-zəm) the unlawful use – or threat – of force or violence against people or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives.**

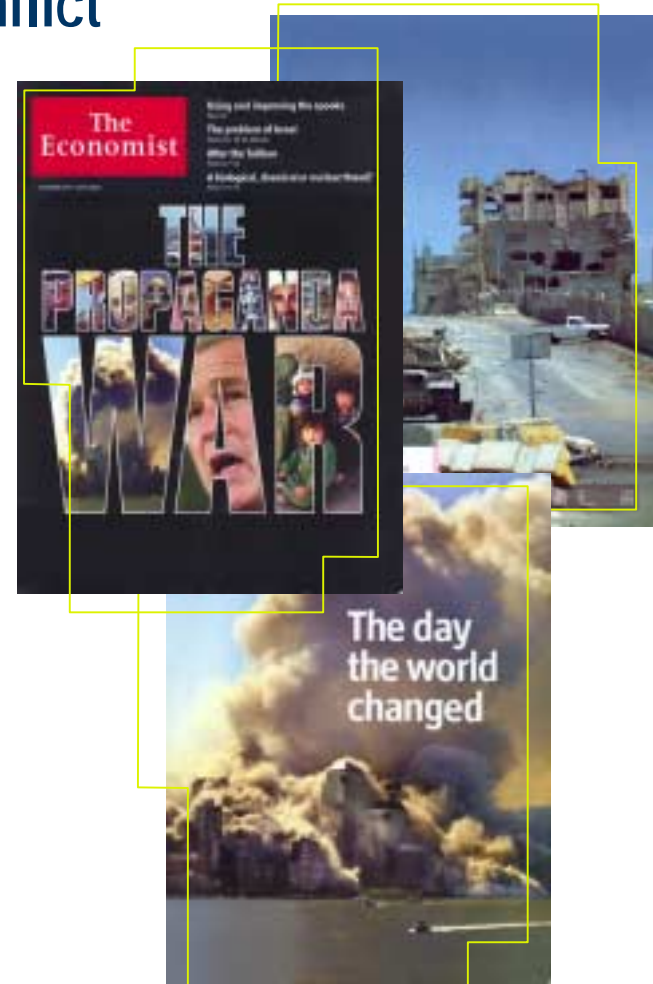
# Terrorism



- Terrorists do not conform to laws of warfare
- Victims are often noncombatants, symbolic persons and places, and political/military figures
- Victims may have no role in either causing or correcting a terrorist's grievance
- Methods include:
  - ▶ Hostage taking
  - ▶ Hijacking
  - ▶ Assassination
  - ▶ Arson
  - ▶ Bombings
  - ▶ Seizures
  - ▶ Hoaxes
  - ▶ Raids
  - ▶ Use of WMD

# Nature of Terrorism

- Not limited to the early stages of a conflict
- Can/probably occur in any level of conflict
- Tactics are described as:
  - ▶ Elusive
  - ▶ Surprising
  - ▶ Brief violent actions



# Common Strategies and Tactics



- Common strategy – commit acts of violence
- Draw attention to “the cause”
- Media plays a crucial part in their strategy
  - ▶ Media gives terrorists recognition
  - ▶ This kind of attention tends to incite acts of violence by other terrorists



# Common Strategies and Tactics



- Victims of the terrorist are seldom the target
- Targets often include:
  - ▶ The general public
  - ▶ Government
  - ▶ Business sectors



# Common Strategies and Tactics

Common Tactics Terrorists Use Include:



- Bombing
- Arson
- Hijacking
- Ambush
- Kidnapping
- Hostage taking
- Assassination
- Other tactics



# Managing Risk in Today's Work Environment

## Introduction



# Goal



To provide a brief overview of a systems approach to risk management when performing security activities related to the protection of people, information, activities, and property

# Preparing Security for the Future



- Provide an understanding of basic risk management concepts and principles
- Show how risk management concepts and methodology are being applied
- Discuss challenges and issues related to the application of the risk management process to security programs

# Security Initiatives

In order to meet these new challenges, risk management has been endorsed by:



- **The Joint Security Commission Report**
- **Presidential Decision Directive/NSC-29**
- **National Security Council/Security Policy Board Risk Management Strategy**

# These Policy Initiatives Share Four Objectives:



- Security policies and services must realistically match the threats and must be flexible to facilitate change as threats evolve
- Security standards and procedures must be consistent and enable us to allocate resources effectively
- Security standards and procedures must result in fair and equitable treatment of all whom we rely on to protect and serve
- Security policies, practice, and procedures must provide the security we need at a price we can afford

# What Should Policies and Procedures Do?



- Provide a range of countermeasure options vs a single “all or nothing” recommendation
- Develop an analytical mindset vs a checklist mentality
- View the customer as a valued contributor to the process of protecting assets vs a captive audience
- Provide value-added security services vs imposing unnecessary or outdated security practices



# Questions? Comments?

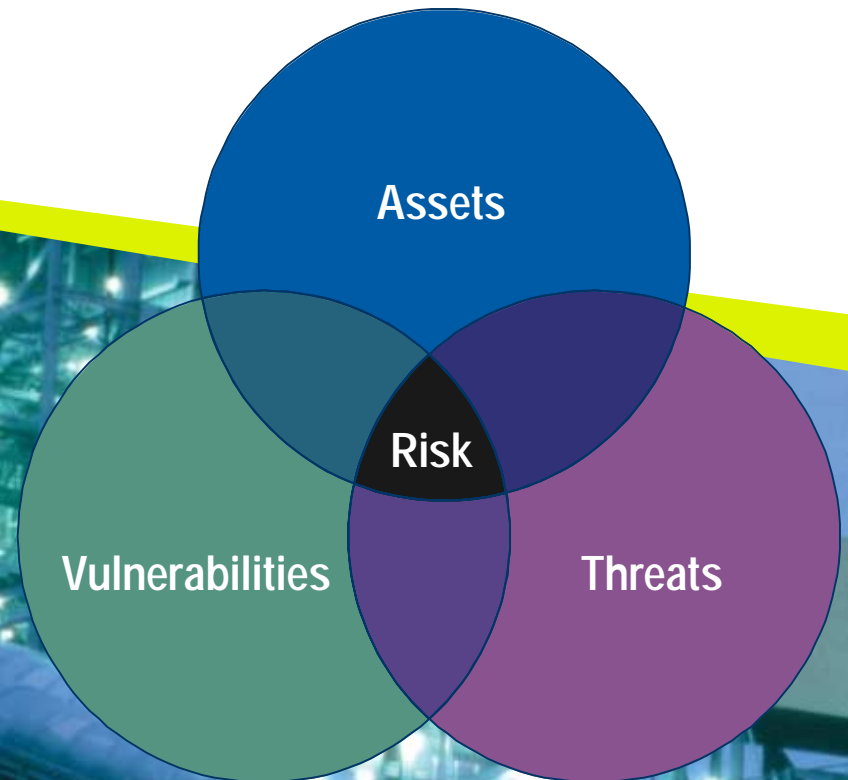
Discussion of Introduction





# Managing Risk in Today's Work Environment

## Key Terms and Definitions



# What is Risk Management?



**The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost**

# What is Risk?



**Risk is the potential for damage or loss of an asset**

- **The level of risk is a combination of two factors**
  - ▶ The value placed on that asset by its owner and the consequence, impact, or adverse effect of loss or damage to that asset
  - ▶ The likelihood that a specific vulnerability will be exploited by a particular threat

# What is an Asset?



**An asset is anything of value (people, information, facilities, activities, equipment, capabilities, etc.)**

# What is Impact?



**Impact is the amount of loss or damage that can be expected, as may be influenced by time or other factors**

# What is Threat?



**Threat is any indication, circumstance, or event with the potential to cause the loss or damage to an asset**

- **Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to your interests**

# What is an Adversary?



**Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to a government or its assets**

- Includes intelligence services, political or terrorist groups, criminals, and private interests

# What are Vulnerabilities?



**Any weakness that can be exploited by an adversary to gain access to an asset**

- **Vulnerabilities can result from, but are not limited to:**
  - ▶ Building characteristics
  - ▶ Equipment properties
  - ▶ Personal behavior
  - ▶ Locations of people, equipment, and buildings
  - ▶ Operational and personnel practices

# What is a Risk Assessment?



**The process of evaluating threat to and vulnerabilities of an asset to give an expert opinion on the likelihood of loss or damage, and its impact as a guide to taking action**

# What is a Cost Benefit Analysis?



Part of the management decision-making process in which the costs and benefits of each alternative are compared and the most appropriate alternative is selected

# Questions? Comments?

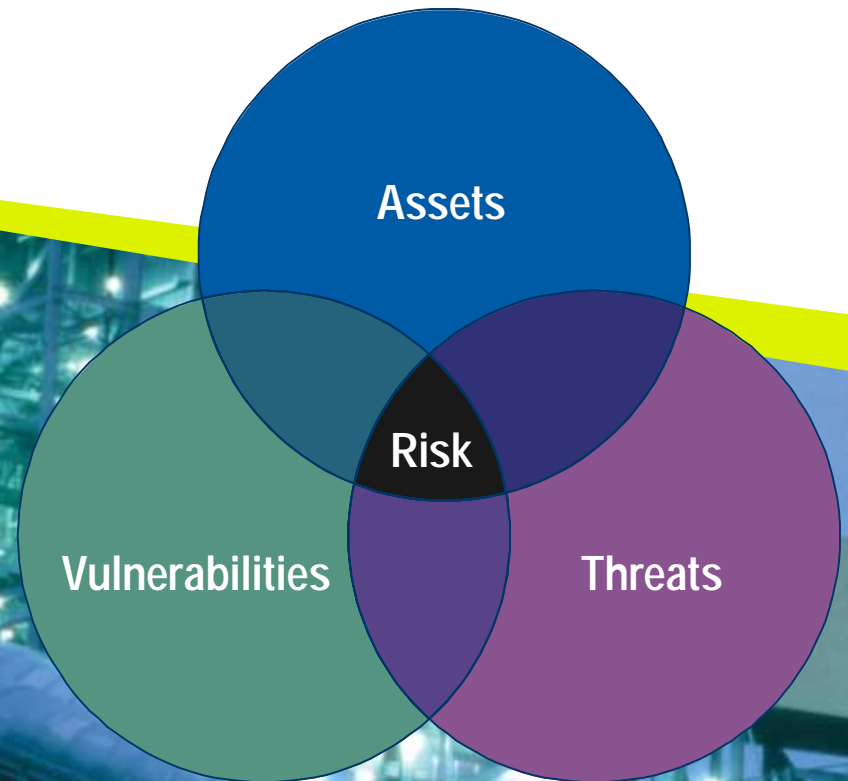
## Discussion of Key Terms and Definitions





# Managing Risk in Today's Work Environment

## Process Overview



# What is Risk Management?



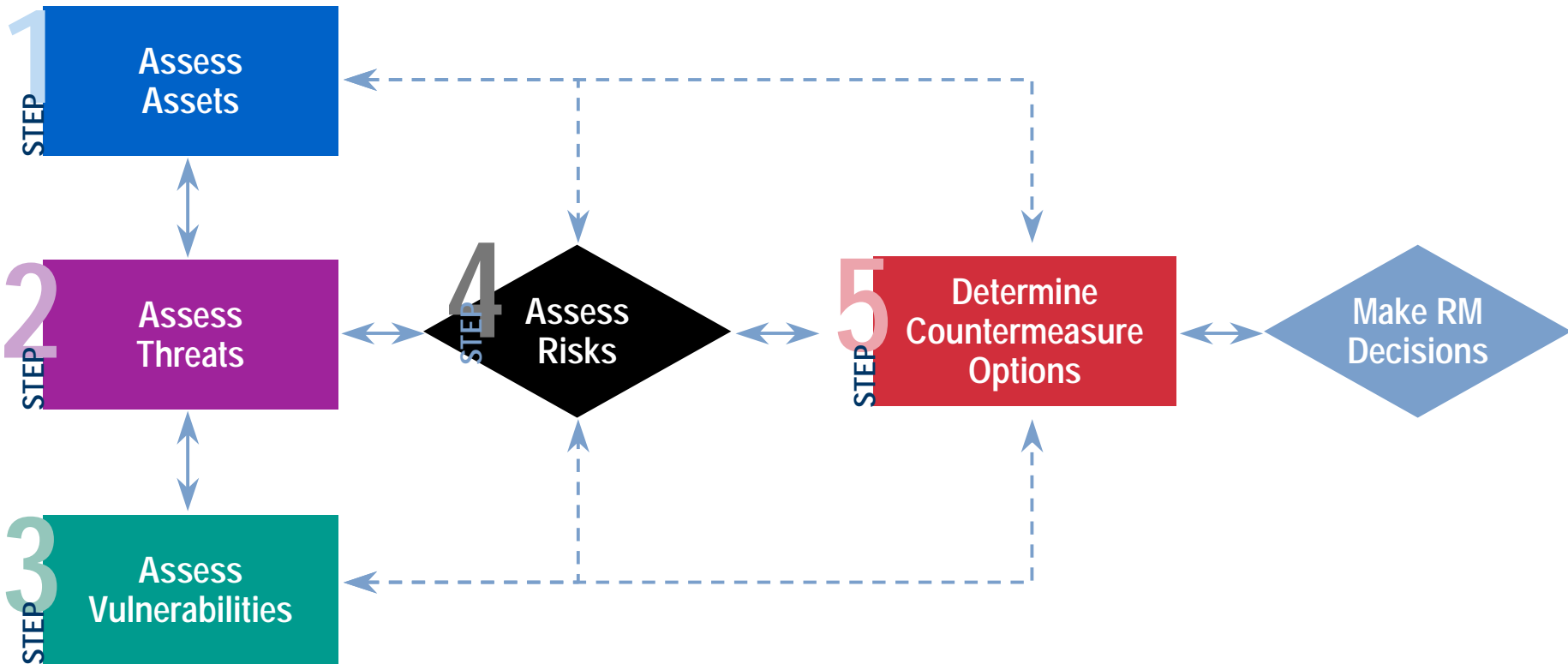
**The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost**

# Risk Avoidance vs. Risk Management



- **Risk avoidance**
  - ▶ Assumes an aggressive, threatening opponent in all scenarios
  - ▶ Counters ALL possible vulnerabilities
  - ▶ Responds to threats based on worst-case scenarios
- **Risk management**
  - ▶ Integrates the process of assessing the threat, the vulnerabilities, and the value of the information to the owner

# The Process at a Glance



# Identify Assets and Loss Impacts



- Determine critical assets requiring protection
- Identify undesirable events and expected impacts
- Value/prioritize assets based on consequences



# What is an Asset?



**An asset is anything of value (people, information, facilities, activities, equipment, capabilities, etc.)**

# Unwanted Event Policy and Procedures

Some Examples:



Loss due to unwanted event		
Massive loss of life	due to	vehicle bombing
Limited loss of life	due to	package bombing
Possible death or injury	due to	letter bomb or intro of substance
Extensive loss of info	due to	employee espionage
Minor loss of info	due to	accidental disclosure
Minor loss of info	due to	collection of emanations
Immobilization of VIP convoy	due to	demonstrations
Loss of documents	due to	surreptitious entry
Destruction of valuable tools	due to	massive flooding

# Identify and Characterize the Threat



- Identify threat categories and adversaries
- Assess intent and motivation of each adversary
- Assess capability of each adversary
- Determine frequency of past incidents
- Estimate threat relative to each critical asset



# Threats and Adversaries



- **What is a threat?**
  - ▶ Any indication, circumstance, or event that can cause the loss of, damage to, or the denial of an asset
- **Who is an adversary?**
  - ▶ Any entity that conducts, or has the capability and intention to conduct, activities detrimental to your interests or assets

# Types of Threats



- **Foreign intelligence services**
  - ▶ Facility penetration
  - ▶ Non-access attack
- **Terrorist threats**
  - ▶ Kidnapping
  - ▶ Bombing
  - ▶ Sabotage
- **Natural threats**
  - ▶ Fire
  - ▶ Flood
  - ▶ Wind (storm, hurricane)
  - ▶ Earthquake
- **Criminal threats**
  - ▶ Fraud, theft, robbery
  - ▶ Arson
  - ▶ Vandalism
  - ▶ Computer hacking
- **Insider threats**
  - ▶ Espionage
  - ▶ Misuse of equipment
  - ▶ Malicious acts by disgruntled staff
- **Military threats**
  - ▶ War
  - ▶ Insurrection
  - ▶ Military action

# We Analyze Threat Data to Understand the Adversary's:



- |   |                   |
|---|-------------------|
| <ul style="list-style-type: none"><li>• Goals</li><li>• Strategy</li></ul>  | Intent            |
| <ul style="list-style-type: none"><li>• Collection/action capability</li><li>• Necessary skills/resources</li></ul> | Capability to Act |
| <ul style="list-style-type: none"><li>• History of successful attacks</li><li>• History of attempts</li></ul>       | History           |

# Analyzing the Intent of Groups and Organizations



Categories	Adversaries	Goals	Strategies
Terrorists*	<ul style="list-style-type: none"> <li>• Hizballah</li> <li>• HAMAS</li> <li>• IRA</li> <li>• Al-Qaeda</li> </ul>	<ul style="list-style-type: none"> <li>• Force change</li> <li>• Gain publicity for the cause</li> </ul>	<ul style="list-style-type: none"> <li>• Conduct bombings and assassinations</li> <li>• Issue threats</li> <li>• Enter negotiations</li> </ul>
Corporate Competitors	Any foreign or domestic competitor	<ul style="list-style-type: none"> <li>• Capture market share</li> <li>• Gain advantage</li> <li>• Make money</li> </ul>	<ul style="list-style-type: none"> <li>• Gather proprietary information legally</li> <li>• Gather proprietary information illegally</li> <li>• Exploit competitor information</li> </ul>
Narco-traffickers	<ul style="list-style-type: none"> <li>• Cali Cartel</li> <li>• Medellin Carte</li> <li>• Others</li> </ul>	<ul style="list-style-type: none"> <li>• Continue business</li> <li>• Stay out of jail</li> <li>• Make money</li> </ul>	<ul style="list-style-type: none"> <li>• Intimidate politicians and law enforcers</li> <li>• Co-opt key politicians and law enforcers</li> </ul>

# Putting it All Together



This threat chart can be use to organize and track the information obtained during the earlier steps

<b>Adversary</b> Insider, Terrorist FIS, Criminal	<b>Intent</b> Interest/Need	<b>Capability</b> Methods	<b>History</b> Incidents/Indicator	<b>Overall Threat Level</b>
Adversary 1	High	High	Yes	High
Adversary 2	Medium	Medium	Yes	Medium
Adversary 3	Low	Medium	No	Low

# Threat Assessment Chart



Critical Assets	Potential Undesirable Events	Threat Category	Threat Rating
People	<ul style="list-style-type: none"> <li>• Assassination due to motorcade attack</li> <li>• Kidnapping of employees/dependants</li> </ul>	Terrorist Terrorist	Medium Medium
Activities and Operations	<ul style="list-style-type: none"> <li>• Disruption of R&amp;D activities</li> <li>• Disruption of communications</li> </ul>	FIS/Insider FIS/Insider	High Medium
Information	<ul style="list-style-type: none"> <li>• Compromise of data</li> <li>• Disclosure of identity/affiliation due to poor tradecraft</li> <li>• Surreptitious entry into R&amp;D lab</li> </ul>	FIS/Insider FIS FIS	High High High
Facilities	<ul style="list-style-type: none"> <li>• Bio-chemical attack</li> <li>• Mail bomb</li> <li>• Vandalism</li> </ul>	Terrorist Terrorist Criminal	Low High Low
Equipment	<ul style="list-style-type: none"> <li>• Theft of computer equipment</li> <li>• Technical implant</li> </ul>	Criminal FIS/Insider	Medium High

# Identify and Analyze Vulnerabilities



- Identify potential vulnerabilities related to specific assets or undesirable events
- Identify existing countermeasures and their levels of effectiveness in reducing vulnerabilities
- Estimate degree of vulnerability to each asset and threat



# What are Vulnerabilities?



**Any weakness that can be exploited by an adversary to gain access to an asset**

- **Vulnerabilities can result from, but are not limited to:**
  - ▶ Building characteristics
  - ▶ Equipment properties
  - ▶ Personal behavior
  - ▶ Locations of people, equipment, and buildings
  - ▶ Operational and personnel practices

# Vulnerability Assessment Chart



Critical Assets	Potential Undesirable Events	Threat Rating	Number Rating	Vulnerability Rating
People	• Assassination due to motorcade attack	Medium	.45	High
	• Kidnapping of employees/dependants	Medium	.39	High
Activities and Operations	• Disruption of R&D activities	High	.55	Medium
	• Disruption of communications	Medium	.37	Medium
Information	• Compromise of data	High	.53	Low
	• Disclosure of identity/affiliation due to poor tradecraft	High	.70	Medium
	• Surreptitious entry into R&D lab	High	.50	Critical
Facilities	• Bio-chemical attack	Low	.13	Critical
	• Mail bomb	High	.67	Low
	• Vandalism	Low	.15	High
Equipment	• Theft of computer equipment	Medium	.37	Critical
	• Technical implant	High	.70	High

# Assess Risks



- Estimate degree of impact relative to each critical asset
- Estimate likelihood of attack by a potential adversary or threat
- Estimate likelihood that a specific vulnerability will be exploited
- Determine relative degree of risk
- Prioritize risks based on integrated assessment



# Assess the Risks



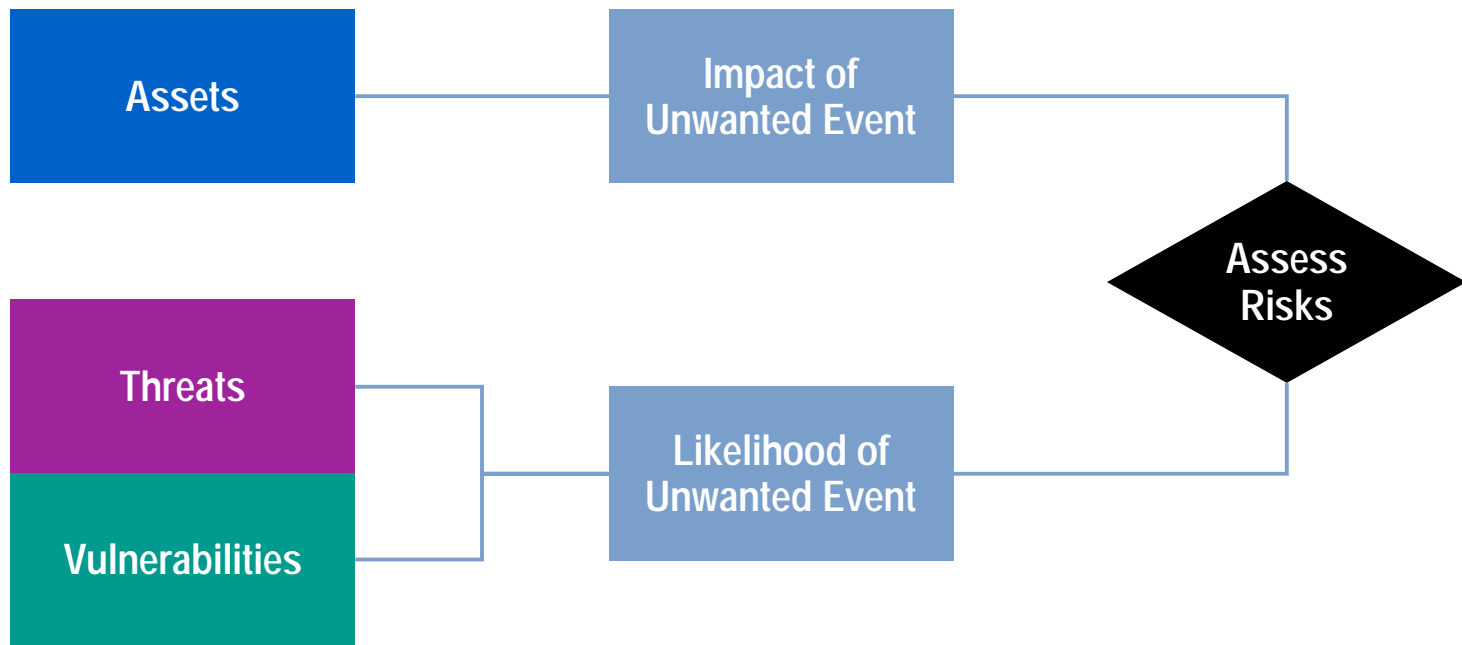
**Risk = Asset x Threat x Vulnerability**

- Quantify the likelihood that an undesirable event will occur
- Determine the severity of the outcome of an undesirable event
- Prioritize the risks

# Risk Formula



**Risk = Impact x Threat x Vulnerability**





# Assess Risk and Determine Priorities for Asset Protection



Critical Assets	Potential Undesirable Events	Asset Rating	#	Rating	Threat Rating	#	Rating	Vuln. Rating	#	Rating	Risk Rating
People	• Assassination due to motorcade attack	Critical	97		Medium	.45		High	.55		High/24
	• Kidnapping of employees/dependants	Critical	88		Medium	.39		High	.75		High/25
Activities and Operations	• Disruption of R&D activities	Medium	.30		High	.55		Medium	.37		Low/.06
	• Disruption of communications	Medium	1		Medium	.37		Medium	.26		Low/.1
Information	• Compromise of data	High	9		High	.53		Low	.24		Med/1.1
	• Disclosure of identity/affiliation due to poor tradecraft	High	4		High	.70		Medium	.28		Med/.8
	• Surreptitious entry into R&D lab	High	8		High	.50		Critical	.87		High/3.5
Facilities	• Bio-chemical attack	Low	100		Low	.13		Critical	1.00		High/13
	• Mail bomb	High	10		High	.67		Low	.15		Med/1
	• Vandalism	Low	.1		Low	.15		High	.70		Low/.01
Equipment	• Theft of computer equipment	Medium	.4		Medium	.37		Critical	.80		Low/.1
	• Technical implant	High	20		High	.70		High	.70		High/9.8

# Identify Countermeasures, Costs, and Benefits



- Identify potential countermeasures to reduce vulnerabilities
- Identify countermeasure benefits in terms of risk reduction
- Identify countermeasure costs
- Conduct countermeasure cost-benefit and tradeoff analyses
- Prioritize options and prepare a recommendation for decision maker



# Countermeasure Costs and Benefits



- **Countermeasures**
  - ▶ An action taken or a physical entity used to reduce or eliminate one or more vulnerabilities
- **Cost-Benefit analysis**
  - ▶ The part of the risk management decision-making process in which the costs and benefits of each countermeasure option are compared and the most appropriate alternative is selected
  - ▶ **Cost:** Includes not only the cost of tangible materials, but also the on-going operational costs associated with countermeasure implementation
  - ▶ **Benefit:** Expressed in terms of the amount of risk reduction based on the overall effectiveness of the countermeasures with respect to the assessed vulnerabilities

# Countermeasure Options



Undesirable Events	Countermeasures	Risk Level Reduced From/To	Threat Rating
Surreptitious Entry	<ul style="list-style-type: none"> <li>• Guards</li> <li>• Doors, locks, bars</li> </ul>	High to Low	\$100,000 \$50,000
Documents Stolen/Mishandled	Security awareness briefing	Medium to Low	Minimal
Kidnapping/ Assassination	Move government official residence to station	Low to Very Low	\$10,000
Terrorist Bomb Attack	<ul style="list-style-type: none"> <li>• Emergency procedures</li> <li>• Fences/barriers</li> </ul>	High to Medium	\$15,000 \$90,000
	Overall Risk/Total Cost	Medium to Low	\$220,000

# What We Want You to Remember



- Analytical risk management is a structured approach to understanding your security posture
- Analytical risk management can help instate reasonable, cost-effective security countermeasures
- Analytical risk management is an iterative process
- Manage the risk
- Think and listen

# Questions? Comments?

## Discussion of Process Overview

