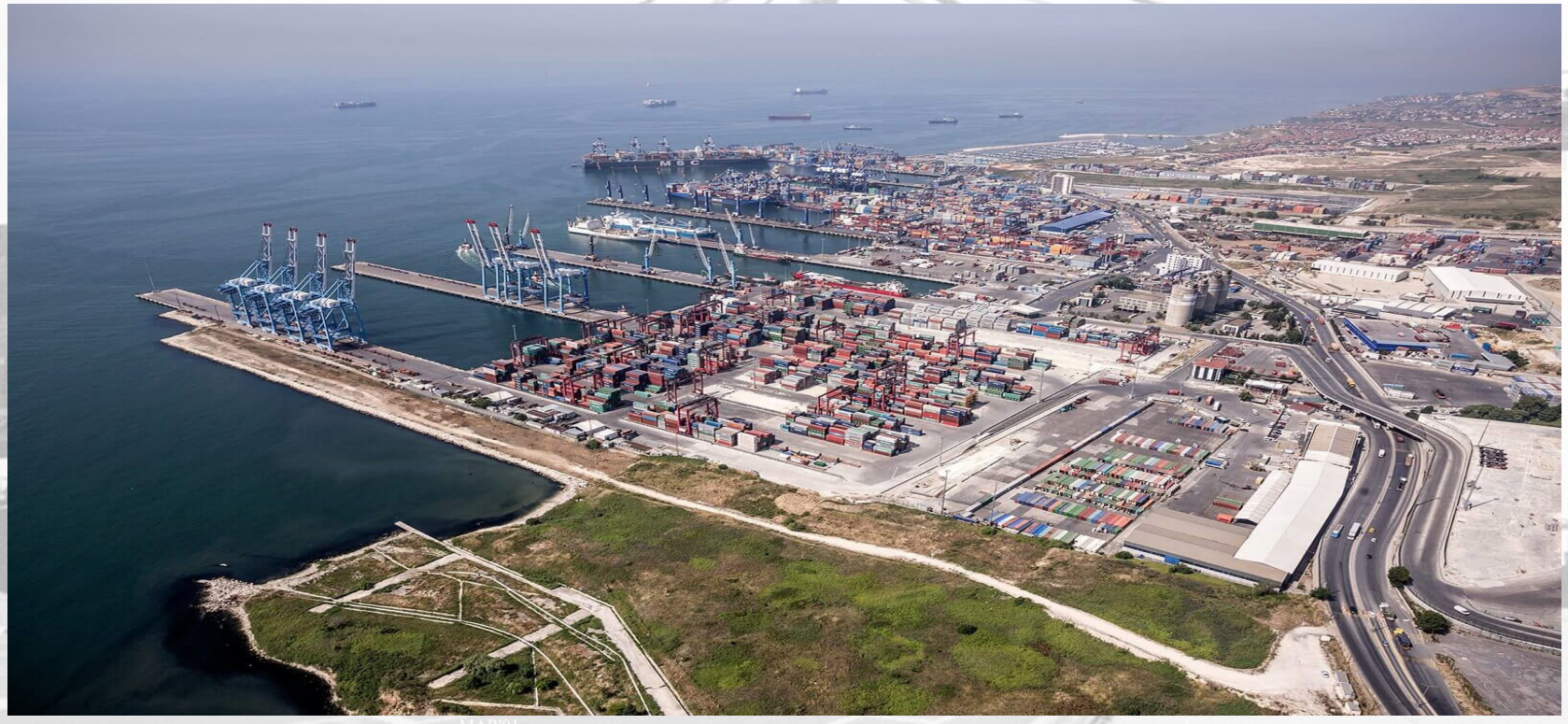
Port Security Management



MAR'01

Risk Management

Lesson Topics

- Quantification of risk
- Identification of threats
- Analyzing consequences
- Assessing vulnerabilities
- Developing mitigation measures
- Reassessment and improvement

Risk Management

Risk is defined as "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk Management

Risk management is an ongoing process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level.

Activities include prevention, mitigation, adaptation or sharing.

It often includes trade-offs between costs and benefits of risk reduction and a choice of a level of tolerable risk.

Risk Management

- **Risk assessment** is a snapshot in time of the risks facing the organization.
- Systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge.

Risk Management

Quantifying Risk

A widely accepted understanding of risk is depicted by the following formula:

Threat ✖ Vulnerability ✖ Consequence = Risk

OR

Criticality ✖ Vulnerability ✖ Probability = Risk

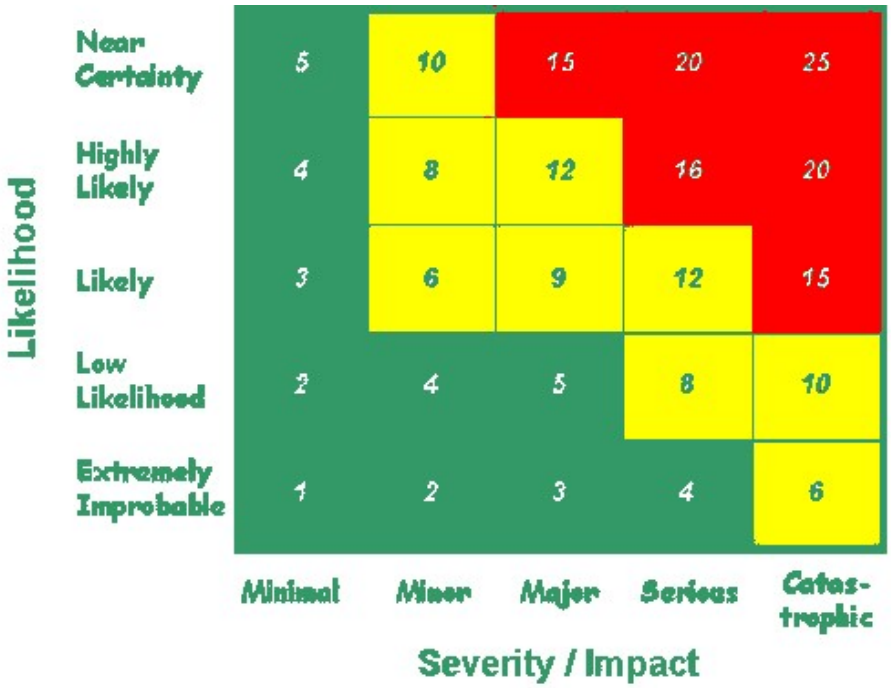
Risk Management

After the threats have been considered by the Port Security Committees or evaluated by intelligence sources as realistic, the ways to reduce risks is to reduce the Vulnerability, or change the impact from Consequence, or both.

Threat ✖ Vulnerability ✖ Consequence = Risk

Risk Management

Risk Quantification



Risk Value Legend
Low: ≤ 5 – Green
Med: >5, ≤ 12 – Yellow
High: > 12 – Red

Risk Management

By employing sound risk management techniques at port facilities, you can reduce the risk to those facilities.

Risk Management

Risk management practices involve an analysis of risks and identification or development of measures to reduce those risks – or in other words, develop measures to counter the threat.

Risk Management

Risk Management involves the following steps:

1. Identify Threats
2. Assess Consequences
3. Assess Vulnerabilities
4. Develop Mitigating/Counter measures
5. Implement Mitigation Measures

Risk Management

1. Identify Threats

- Consider attack scenarios
- Be realistic
- These should be consistent with the Port Facility Security Assessment and Port Facility Security plan
- Avoid assessing an excessive number of similar scenarios

Risk Management

2. Assess Consequences

- Determine the consequence level (e.g. High, Medium, Low) for each scenario
- The consequence level should be consistent with the type of facility (e.g. a facility that handles dangerous cargo should have a higher consequence than one that does not)

Risk Management

3. Assess Vulnerabilities

- Determine the facility's vulnerability to each attack scenario
- Assign vulnerability rating (e.g. High, Medium, Low) for each scenario
- Consider 4 factors in determining degree of vulnerability

Risk Management

Vulnerability Factors:

- Availability
- Accessibility
- Organic security
- Facility hardiness

Risk Management

Vulnerability Assessment: Availability

The facility's presence and predictability as it relates to the nature of the attack.

Risk Management

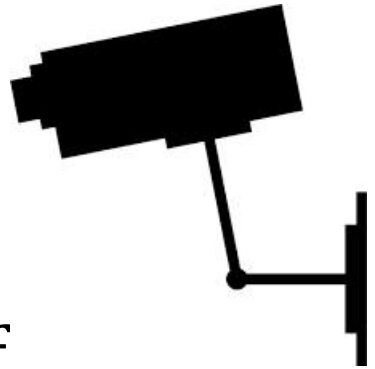
Vulnerability Assessment: Accessibility

Accessibility of the facility to the attack scenario. This relates to the physical and geographic barriers that deter the threat without organic security.

Risk Management

Vulnerability Assessment: Organic Security

- The ability of security personnel to deter the attack
- Security plans, communication capabilities, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent the attack.



Risk Management

Vulnerability Assessment: Facility Hardiness

- The ability of the facility to withstand the specific attack based on the complexity of facility design and material construction characteristics.

Risk Management

4. Develop Mitigation Strategy

- Determine which scenarios require mitigation strategies based on degree of Vulnerability and Consequence
- Document the mitigation strategies in the Port Facility Security Plan

Risk Management

5. Implement Mitigation Strategy

- Procure necessary equipment, systems, or resources
- Develop and implement processes and procedures
- Conduct training to prepare personnel to implement processes and procedures

Risk Management

Tactical Time

- **Short time horizon – immediate action required– e.g., deploy police to thwart intelligence-identified attack plan**
- **Defender seeks to interrupt attackers' decision-action loop**
- **Response directly informed by our best knowledge of the situation**

Strategic Time

- **Long time horizon - deliberate action planned– e.g. build a new facility or upgrade existing capital security features**
- **Attacker can go through their decision-action loop many times**
- **Long-term *probability* is unknown and extremely uncertain**

Risk Management

Risk Management should be a continual process.

- Threats are continuously identified
- Vulnerability determinations are continually refined
- Mitigation strategies are continually refined

Continuous Improvement

Port Directors, Port Security Officers, Port Facility Security Officers, and all members of the Port Security Department should strive to conduct continuous improvement in the port security posture of port facilities.

Continuous Improvement

The primary sources for lessons learned are:

- Drills
- Exercises
- Training
- Security Incidents

Summary

Risk management is the process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level, considering associated costs and benefits of any actions taken.

Summary

There is an optimal balance where security and operations should reached to ensure products and services are delivered by the port facility and vessels

Summary

A widely accepted understanding of risk is depicted by the following formula:

Threat ✖ Vulnerability ✖ Consequence = Risk

Summary

Risk Assessment involves the following steps:

1. Identify Threats
2. Assess Consequences
3. Assess Vulnerabilities
4. Develop Mitigation Strategy
5. Implement Mitigation Measures

Summary

The primary sources for lessons learned are:

- Drills
- Exercises
- Training
- Security Incidents