



# Security Risk Assessment - Protection of Industrial Concerns Against Terrorism

Presenter: Naseeruddin Humayun



# Scope

- ◆ Purpose
- ◆ Terminology
- ◆ Seven Steps to General Security Risk Assessment
- ◆ Process Flow Chart
- ◆ Loss Event Information Sources
- ◆ Qualitative Approach
- ◆ Quantitative Approach



# Purpose

To provide you with a simple step-by-step methodology by which security risks at any specific location can be identified, appropriately solved and communicated.



# Terminology

- ◆ **Assets.** Any real or personal property, tangible or intangible, owned by a company/individual that can be assigned a monetary value.
- ◆ **Consequential.** Any secondary result ensuing from an action or decision.
- ◆ **Criticality.** Impact of a loss event – calculated as net cost of that event.
- ◆ **Cost/Benefit Analysis.** A process in planning, related to the decision to commit funds or assets. Involves 3 systemic steps:
  - ID of all in/direct consequences of expenditure.
  - Assignment of monetary value
  - Discounting effected future costs & revenues to express as current monetary values.
- ◆ **Events.** Noteworthy happening – such as security incident, theft, fire, medical emergency.
- ◆ **Loss Event.** An occurrence that actually produces a financial loss or negative impact on assets.



# Terminology cont..

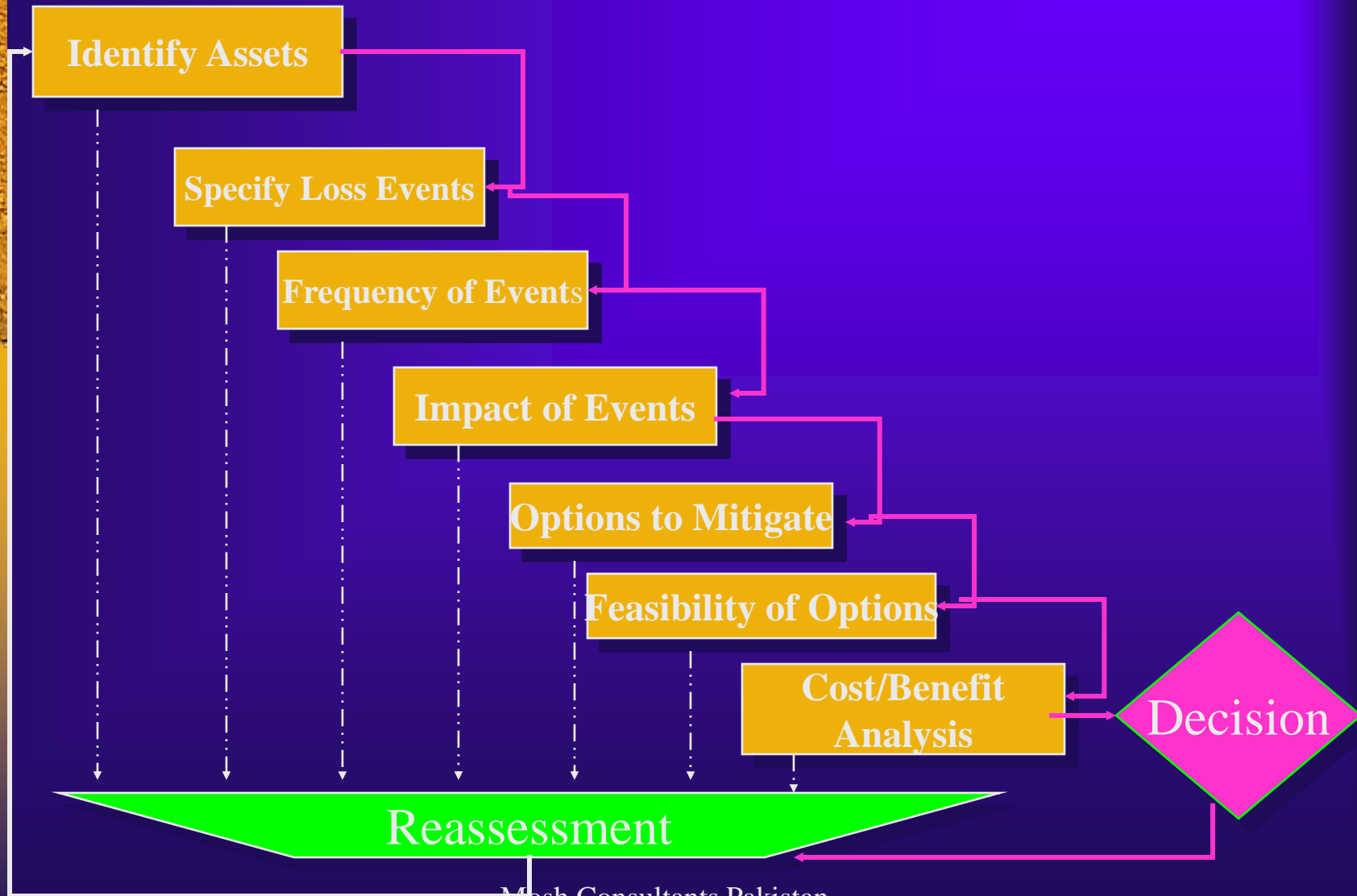
- ◆ **Goodwill.** The value of a business that has been built up through the reputation of the business concern and its owners.
- ◆ **Probability.** The chance or mathematical certainty that a given event will occur.
- ◆ **Qualitative.** Relating to that which is characteristic of something and which makes it what it is.
- ◆ **Quantitative.** Relating to, concerning, or based on the amount/number of something, capable of being measured or expressed in numerical terms.
- ◆ **Risk.** The possibility of loss resulting from a threat, security incident or event.
- ◆ **Vulnerability.** An exploitable capability/ security weakness or deficiency at a facility, venue or of a person.
- ◆ **Threat.** An intent of damage or injury; an indication of something impending.



# Seven Steps to General Security Risk Assessment

1. Understand the organisation & ID people and assets at risk.
2. Specify loss risk events/vulnerabilities.
3. Establish the probability of loss risk & frequency of events.
4. Determine the impact of the events.
5. Develop options to mitigate risks.
6. Study the feasibility of options implementation.
7. Perform a cost/benefit analysis

# Risk Assessment Process Flow Chart





# Loss Events Information Sources

1. Local police crime statistics.
2. Crime reports or comparable data.
3. Company internal documents such as security management info.
4. Prior complaints from employees, customers, guests, visitors, etc.
5. Prior civil claims for inadequate security measures.
6. Intelligence from law enforcement agencies about potential threats
7. Industry-related information about trends.
8. General economic conditions of the area.
9. Presence of a crime magnet (popular night club, presence of vagrants, property in disrepair).



# Qualitative Approach:

## Step 1 Practice Advisory

### “Understand the organisation”

#### COMMENTARY-

The security practitioner should understand the complexities and nuances of how the organisation operates. Should obtain the following types of info:

- ◆ Hours of operation for each department.
- ◆ Staffing levels during each shift.
- ◆ Types of service provided and/or goods produced.
- ◆ Type of clientele served.
- ◆ The competitive nature of the business enterprise.
- ◆ Special issues raised by the manufacturing process (waste).
- ◆ Type of labour used.



# Qualitative Approach:

## Step 1 Practice Advisory cont..

### “Identify the people and assets at risk”

#### COMMENTARY-

**People** – Included employees, customers, visitors, vendors, patients, guests, passengers, tenants, contractors and any other persons who are lawfully present on company property.

**Property** – **(1) Tangible property** includes real estate, land, buildings, facilities, high theft items, anything that can be stolen, damaged or otherwise adversely affected by a loss event. **(2) Core business**, goodwill or reputation. **(3) Information** such as proprietary data, trade secrets, marketing plans, intellectual property, etc. **(4) Networks** include all systems, infrastructure and equipment associated with data, telecommunications and computer processing assets.



# Qualitative Approach:

## Step 2 Practice Advisory

### “Specify loss risk events/vulnerabilities”

#### COMMENTARY –

Loss Event Main Categories:

#### ◆ **Crime-Related Events:**

- Local police crime statistics for 3-5 year period.
- Uniform crime reports for the municipal area.
- Demographic/social condition data (economic conditions, population densities, unemployment rates, etc.)
- Prior criminal and civil complaints brought against company.
- Intelligence from local/ state/federal law enforcement agencies which can affect the company.
- Professional groups and associations that share data on industry-specific problems or trends in criminal activity.
- Other environmental factors such as climate, site accessibility and presence of crime-magnets.



# Qualitative Approach: Step 2 Practice Advisory cont..

## ◆ **Non-Criminal Events:**

- **Natural disasters** include hurricanes, major storms, earthquakes, lightning strikes and fires caused by natural disasters.
- **Man-made disasters** includes labour strikes, airplane crashes, vessel collisions, power failures, depletion of essential resources.

- ◆ **Consequential Events** — Through a relationship between events or between two companies, the company suffers some type of loss as a consequence. Example: When one organisation engages in illegal activity or produces a harmful product it could taint the reputation of an innocent company by virtue of it's affiliation alone.



# Qualitative Approach: Step 3 Practice Advisory


## “Establish the Probability of Loss Risk”

### COMMENTARY

Probability of loss not based on mathematical certainty. It is consideration of the likelihood that a loss risk event may occur in future based upon:

- Historical data,
- history of like events at similar enterprises,
- nature of the neighbourhood,
- immediate vicinity,
- overall geographical location,
- political and social conditions and
- changes in the economy.

Degree of probability will affect the decision-making process in determining the appropriate solution to be applied to the potential risk exposure.



# Qualitative Approach: Step 3 Practice Advisory cont... “Establish the Frequency of Events”

## COMMENTARY

The Practitioner should query how often an exposure exists per event type. The frequency of each event has to be determined independently.

# Qualitative Approach:

## Step 4 Practice Advisory

### “Determine the Impact of the Event”

#### COMMENTARY

The Practitioner should consider all potential costs or less obvious ways in which loss risk events impact on the business. Even when the probability of loss is low but the impact costs are high, security safeguards still are necessary to manage the risk.

#### Direct Costs include:

- ◆ Financial losses associated with the event – value of goods stolen.
- ◆ Increased insurance premium for several years after a loss.
- ◆ Deductible expenses on insurance coverage.
- ◆ Lost business from an immediate post-risk event – stolen can't be sold.
- ◆ Labour expenses incurred resulting from the event – increase in security.
- ◆ Management time dealing with the disaster/event – media liaison.
- ◆ Punitive damages awards not covered by ordinary insurance.

# Qualitative Approach:

## Step 4 Practice Advisory cont...

### “Determine the Impact of the Event”

#### Indirect Costs include:

- ◆ Negative media coverage.
- ◆ Long-term negative consumer perception.
- ◆ Additional public relations costs to overcome poor image problems.
- ◆ Lack of insurance coverage due to a higher risk category.
- ◆ Higher wages needed to attract future employees due to negative perceptions about the business.
- ◆ Shareholder derivative suits for mismanagement.
- ◆ Poor employee morale, causing to work stoppages, higher turnover, etc.





# Qualitative Approach: Step 5 Practice Advisory “Develop Options to Mitigate”

## COMMENTARY

In theory the Practitioner will have a range of options available to address loss events faced by the business. In practice some options may not be feasible or too costly. Options include:

- ◆ Risk Reduction – security procedures, equipment & staff).
- ◆ Risk Transfer – via insurance coverage or contract terms.
- ◆ Risk Avoidance – terminating this part of business.
- ◆ Risk Acceptance – regard risk as cost of doing business.

Option chosen still must be evaluated in terms of availability, affordability, and feasibility of application to the enterprise’s operation.



## Qualitative Approach: Step 6 Practice Advisory “Study the Feasibility of Option Implementation”

### COMMENTARY

The practical considerations of each option should now be taken into account.

While financial cost is often a factor, a common consideration is whether the strategy will interfere substantially with the operation of the business.

The challenge for the Security Practitioner is to strike that balance between a sound security strategy and consideration of the operational needs of the business, as well as the psychological impact on the people affected by the security program.



## Qualitative Approach: Step 7 Practice Advisory “Perform a Cost/Benefit Analysis”

### COMMENTARY

The final step is consideration of the cost versus benefit of a given security strategy.

Weigh the actual cost of security program implementation against the impact of the loss, financially and otherwise.

Makes no sense to spend \$150'000 on security equipment to prevent the theft of a \$1'500 item. It could make more sense to take out insurance on the item or remove it to a more secure location.

# Thank You

- ◆ I would now welcome Questions, if any!