Chapter 2 – Risk Strategies Simple Risk
Simple Risk Definitions

- **Risk**: potential for an unwanted outcome.
- **Risk Assessment**: product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.
- **Risk Assessment Methodology**: set of methods, principles, or rules used to identify and assess risks and to form priorities, develop courses of action, and inform decision-making.
- **Risk Management**: process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost.

Simple Risk Definitions (Cont.)

- **Risk management Cycle**: sequence of steps that are systematically taken and revisited to manage risk.
- **Risk Management Methodology**: set of methods, principles, or rules used to identify, analyze, assess, and communicate risk, and mitigate, accept, or control it to an acceptable level at an acceptable cost.
- **Risk Management Plan**: document that identifies risks and specifies actions chosen to manage those risks.
- **Risk Management Strategy**: course of action or actions to be taken in order to manage risks.

Simple Risk Definitions (Cont.)

- **Risk Mitigation**: application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences.

- **Risk Transfer**: action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area.

- **Risk-Informed Decision Making**: determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, as well as other relevant factors.

For Simple Risk in this Class

- Risk = expected loss = Probability x Consequence
- Probability = likelihood of an event
- Consequence = loss in terms of casualties, money, time, deaths, capital, economic damage, and so forth.

Threat: probability of an attack, hazardous event or detrimental incident.

Vulnerability: probability of damage or consequence given a successful attack, hazardous event, or detrimental incident occurs. In simple terms a weakness.

Asset: person, structure, facility, information, material, or process that has value.

Threat-Asset Pair: probability of threat depends on the asset or target of the threat.

Can you link the asset to a known threat and/or recent event?
Example of Threat-Asset Pair

Source: Figure 2.1a in Text
Possibilities of threat in this scenario are a flat tire, running out of gasoline or a stopped car ahead or a combination of 2 or all 3.
Possibilities are that there will be no damage or only one of three possible hazards may occur.

Source: Figure 2.1c in Text
Possibilities are that all 3 hazards must occur in order for the car to be damaged.

Source: Figure 2.1d in Text
Possibilities are that all 3 hazards must occur in order for the car to be damaged.

Source: Figure 2.1d in Text
Risk Analysis

Risk = T x V x C

Where:

- **T** = Threat = Probability of hazard (threat)
- **V** = Vulnerability = Probability of damage
- **C** = Consequences

**Example:**

There is a bomb threat with the probability of occurrence of 0.1; building vulnerability of 0.25 and consequence of $10,000 (in damage).
Example solution:

Risk = 0.1 \times 0.25 \times \$10,000 = \$250

Now, what if you reduced the vulnerability by installing a fence around the building at a cost of \$5000 (E = prevention cost) from 0.25 to 0.01.

Then:

Risk = 0.1 \times 0.01 \times (\$10,000) = \$10
Return on Investment

- ROI = Return on Investment is a measure of the effectiveness of risk reduction:
  \[ \text{ROI} = \frac{\text{Risk(before investment)} - \text{Risk(after)}}{\$\text{Invest}} \]

- Example Continued: The fencing around building cost of $5,000, the Risk(before) is $250 and the Risk(after) is $10. What is the ROI?
  \[ \text{ROI} = \frac{($250 - $10)}{$5000} = $0.048/\$\text{invest or 4.8%} \]
Return on Investment

- ROI = Return on Investment is a measure of the effectiveness of risk reduction:
  \[ \text{ROI} = \frac{\text{Risk(before investment)} - \text{Risk(after)}}{\$\text{Invest}} \]

- Example Continued: The fencing around building cost of $5,000, the Risk(before) is $250 and the Risk(after) is $10. What is the ROI?
  \[ \text{ROI} = \frac{($250 - $10)}{$5000} = \frac{0.048}{\$\text{invest}} \text{ or } 4.8\% \]
## Car Example

- Initial risk is $270 (Table 2.1a in Text)

<table>
<thead>
<tr>
<th>Threat</th>
<th>T</th>
<th>V</th>
<th>C</th>
<th>Elimination Cost</th>
<th>Initial Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flat</td>
<td>50%</td>
<td>50%</td>
<td>$300</td>
<td>$100.00</td>
<td>$75.00</td>
</tr>
<tr>
<td>Gas</td>
<td>80%</td>
<td>50%</td>
<td>$300</td>
<td>$50.00</td>
<td>$120.00</td>
</tr>
<tr>
<td>Stop</td>
<td>25%</td>
<td>100%</td>
<td>$300</td>
<td>$200.00</td>
<td>$75.00</td>
</tr>
<tr>
<td><strong>Total Risk</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>$270.00</strong></td>
</tr>
</tbody>
</table>

- Risk is reduced to $117.83 by distributing $50 in investments among the 3 threats (Table 2.1b in Text)

<table>
<thead>
<tr>
<th>Threat</th>
<th>T</th>
<th>Reduced V</th>
<th>Elimination Cost</th>
<th>Allocation</th>
<th>Reduced Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flat</td>
<td>50%</td>
<td>24.55%</td>
<td>$100</td>
<td>$18.18</td>
<td>$36.83</td>
</tr>
<tr>
<td>Gas</td>
<td>80%</td>
<td>7.67%</td>
<td>$50</td>
<td>$23.96</td>
<td>$18.42</td>
</tr>
<tr>
<td>Stop</td>
<td>25%</td>
<td>83.43%</td>
<td>$200</td>
<td>$7.87</td>
<td>$62.58</td>
</tr>
<tr>
<td><strong>Total Risk</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>$117.83</strong></td>
</tr>
</tbody>
</table>
Risk Analysis with Investment

Risk = T x V(E) x C

Where
- T = probability of hazard
- V(E) = reduced vulnerability probability
- E = $Investment to reduce V
- C = consequence in $

V(E) is an exponentially declining function of E

V(E) = V(0) exp(-gE/E_max)

Where:
- g: constant
- E: $Investment
- E_max: elimination cost - input

Note: V(0) and E_max are input values to the MBRA tools
Fault Tree Optimization

- Fault tree model of hypothetical hospital with redundant power (Figure 2-3 in Text)

- Hospital normally depends on the power grid, but has a backup power source. The grid is vulnerable to mishap and terrorist attacks. The backup power supply is vulnerable to floods (and more?).
Investment is a Resource Allocation Problem

- Input values to the hospital fault tree. (Table 2-2a in Text)

<table>
<thead>
<tr>
<th>Threat</th>
<th>T</th>
<th>V</th>
<th>C</th>
<th>Elimination Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood</td>
<td>50%</td>
<td>50%</td>
<td>$1,000</td>
<td>$100</td>
</tr>
<tr>
<td>Terrorist</td>
<td>50%</td>
<td>50%</td>
<td>$2,000</td>
<td>$1,000</td>
</tr>
<tr>
<td>Mishap</td>
<td>50%</td>
<td>50%</td>
<td>$1,000</td>
<td>$200</td>
</tr>
<tr>
<td>Initial Risk</td>
<td></td>
<td></td>
<td>$1,000</td>
<td></td>
</tr>
</tbody>
</table>

- Optimal allocation of $125^K to reduce risk in the fault tree model (Table 2.2.b in Text).

<table>
<thead>
<tr>
<th>Threat</th>
<th>Allocation</th>
<th>Reduced V</th>
<th>Reduced Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood</td>
<td>$44.00</td>
<td>8.95%</td>
<td>$44.73</td>
</tr>
<tr>
<td>Terrorist</td>
<td>$28.50</td>
<td>44.70%</td>
<td>$447.30</td>
</tr>
<tr>
<td>Mishap</td>
<td>$52.55</td>
<td>17.90%</td>
<td>$89.46</td>
</tr>
<tr>
<td>Reduced Risk</td>
<td>$581.49</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Investment: $125
ROI declines as you spend more to reduce risk due to diminishing returns (Table 2.4 in Text)

Risk and ROI diminish as investment increases, therefore risk tradeoffs are required.
USCG Maritime Security Risk Analysis Method (MSRAM)

- Most successful use of probabilistic risk analysis outside of the nuclear power industry.
- Identify and prioritize critical infrastructure and key resources

\[ \text{Risk} = T \times V \times C \]

Where:
- \( T = \text{Intent} \times \text{Capability} \)
- \( \text{Intent} = \text{Measure of propensity to attack} \)
- \( \text{Capability} = \text{Measure of ability to attack} \)
- \( V = \text{Weakness of target} \)
- \( C = \text{modified consequence based on preventive measures} \)
Risk Analysis with Intelligent Adversary

\[ \text{Risk} = T(A) \times V(E) \times C(D) \]

- This assumes an intelligent adversary that targets weaknesses in the infrastructure, where:
  - \( T(A) \) is an increasing function of threat resources
  - \( A \) are the resources used to increase \( T \)
  - \( C(D) \) is the consequence reduction by response
  - \( D \) is the response budget

\[
T(A) = 1 - \exp(-aA/A_{\text{max}})
\]

- Where:
  - \( a \) is a constant
  - \( A \) is the threat investment to increase \( T \)
  - \( A_{\text{max}} \): assumed to be equal to \( E_{\text{max}} \)
The defender attempts to minimize risk, while an attacker attempts to maximize risk by optimal allocation of threat resources.

Revisiting the hypothetical hospital scenario (Figure 2-5 in Text)
Game Theory Results

- Inputs to MBRA (Table 2-3a. In Text)

<table>
<thead>
<tr>
<th>Node</th>
<th>T</th>
<th>V</th>
<th>C</th>
<th>Prevention Cost</th>
<th>Response Cost</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>0.5</td>
<td>0.5</td>
<td>1000</td>
<td>50</td>
<td>50</td>
<td>250</td>
</tr>
<tr>
<td>Grid</td>
<td>0.5</td>
<td>0.5</td>
<td>3000</td>
<td>600</td>
<td>600</td>
<td>750</td>
</tr>
<tr>
<td>Totals</td>
<td></td>
<td></td>
<td>4000</td>
<td>650</td>
<td>650</td>
<td>1000</td>
</tr>
</tbody>
</table>

- Defender only allocation (Table 2-3b. In Text)

<table>
<thead>
<tr>
<th>Node</th>
<th>T</th>
<th>V</th>
<th>C</th>
<th>Prevent Alloc</th>
<th>Response Alloc</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>0.5</td>
<td>0.32</td>
<td>702</td>
<td>5.77</td>
<td>3.85</td>
<td>111.7</td>
</tr>
<tr>
<td>Grid</td>
<td>0.5</td>
<td>0.32</td>
<td>2105</td>
<td>69.23</td>
<td>46.15</td>
<td>335.1</td>
</tr>
<tr>
<td>Totals</td>
<td></td>
<td></td>
<td>2807</td>
<td>75</td>
<td>50</td>
<td>446.8</td>
</tr>
</tbody>
</table>

- Attacker-Defender allocations (Table 2-3c. in Text)

<table>
<thead>
<tr>
<th>Node</th>
<th>T</th>
<th>V</th>
<th>C</th>
<th>Prevent Alloc</th>
<th>Response Alloc</th>
<th>Attack Alloc</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>0.82</td>
<td>0.18</td>
<td>389</td>
<td>13.3</td>
<td>10.24</td>
<td>21.8</td>
<td>57.4</td>
</tr>
<tr>
<td>Grid</td>
<td>0.56</td>
<td>0.33</td>
<td>2211</td>
<td>61.7</td>
<td>39.80</td>
<td>100.2</td>
<td>408.6</td>
</tr>
<tr>
<td>Totals</td>
<td></td>
<td></td>
<td>2600</td>
<td>75</td>
<td>50.04</td>
<td>122</td>
<td>466</td>
</tr>
</tbody>
</table>

- Prevention cost is the cost to diminish vulnerability and response cost is to minimize consequences.
What is the Model-Based Risk Assessment (MBRA) Technique?

- By textbook description, the MBRA technique is used for modeling critical infrastructure as fault trees and networks. MBRA calculates risks, computes optimal resource allocation and simulates single asset failures and resulting effects on networks. MBRA can be performed by manual calculation, in spreadsheets or via simulations, tools and software.
Finding T, V, and C

- How do you estimate T, V, and C?
  - Ask a subject matter expert
  - Build a model/simulation
    - Blast models vs. buildings
    - Weather models vs. cities
    - Flood/fire, etc. models

- How do you estimate probabilities?
  - T and V are likelihoods, e.g. estimates of chance
  - a priori probability = ratio of outcomes
  - a posteriori probability = historical records
Controversial T

- Is T an input or output value?
  - Some say T is an independent input value
  - Some say T depends on V and C
  - Some say T should be an output from risk analysis

- Bayesian probability approach
  - T is an output that depends on other factors
  - T is a conditional probability
  - Bayesian belief replaces simple probabilities

Note: Bayesian probability theory is a type of a posteriori (knowledge or justification dependent on experience or empirical evidence) probability theory that states the likelihood of an event increases or decreases according to other events.
Bayesian Network

- Bayesian network model of a hypothetical Bomb-Bridge pair (Figure 2-6 in Text).

Where:
- \( T \) depends on \( S \) and \( B \) and increases in \( S \) and \( B \) lead to increases in \( T \)
Simple Risk Summary

- Probabilistic Risk Analysis is the simplest risk model based on expected utility theory.
- T and V are probabilities; C is consequence.
- E, D and A are investments in prevention, response, and attack.
- Thus: Risk = T(A) x V(E) x C(D), can be optimized using game theory, where:
  - Attacker maximizes risk
  - Defender minimizes risk
Simple Risk Summary (Cont.)

- Simple risk is not so simple when considering threat-asset pairs.
- A fault tree model allows flexible probabilistic risk analyses, but has limitations, e.g. diminishing returns.
- ROI can be easily calculated, but acceptable ROI is a policy decision – there is no optimal ROI.
- Fault tree optimizations minimize risk by maximizing ROI for every threat-asset pair.
Chapter 2 – Risk Strategies
System Risk

School of Criminology and Justice Studies
University of Massachusetts Lowell
System Risk Definitions

- **Exceedance Probability**: the probability $E(x \geq X)$ that $x$ equals or exceeds $X$.
- **Ranked Exceedance**: $EP(n \geq N)$ represents the probability that $n$ events equal or exceed $N$.
- **True Exceedance**: $EP(c \geq C)$ represents the probability that the size of an event $c$ equals or exceeds $C$.
- **Probable Maximum Loss (PML)**: the maximum expected loss defined as $PML = EP(c \geq C) \cdot C$.
  - PML replaces PRA as a risk methodology.
Exceedance is Typically Long-tailed

- $E(x \geq X)$ is usually a long-tailed distribution.
  - Most-often obeys a power law
  - Power law: $E(x \geq X) = x^{-q}$
  - $q$ is called the fractal dimension

- **Examples:**
  - Guttenberg-Richter scale for earthquakes (ranked)
  - Power outages from power grid failures (true)
In statistics, a long-tailed distribution is the portion of the distribution that has a large number of occurrences far from the head or central part of the distribution. The distribution could involve popularities and random numbers of occurrences of events with various probabilities.

Source: The Long Tail of Expertise, Bingham and Spradlin (2011)
A probability distribution is said to have a long tail if a larger share of the population (of occurrences) rests within its tail than would under a normal distribution.

A long-tail distribution will arise with the inclusion of many values unusually far from the mean, which increase the magnitude of the skewness (measure of the asymmetry of the probability distribution of a real-valued random variable about its mean) of the distribution.

Earthquakes follow a long-tailed ranked exceedance probability curve (Figure 2-7 in Text).

Example of a ranked exceedance probability curve using the Guttenberg-Richter scale. The number of earthquakes of magnitude M is plotted against M (Richter number). The same data are plotted logarithmically.
Low vs. High PML Risk

- PML risk depends on fractal dimension, q (Figure 2-8 in Text).
Examples

- Fractal dimensions of some hazards (Table 2-4 in Text)

Risk = $C^{1-q}$

<table>
<thead>
<tr>
<th>Asset/Sector</th>
<th>Consequence</th>
<th>Exponent Low Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large Fires in Cities</td>
<td>$Loss$</td>
<td>2.1</td>
</tr>
<tr>
<td>Airline Accidents</td>
<td>Deaths</td>
<td>1.6</td>
</tr>
<tr>
<td>Tomatoes</td>
<td>Deaths</td>
<td>1.4</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Deaths</td>
<td>1.4</td>
</tr>
<tr>
<td>Floods</td>
<td>Deaths</td>
<td>1.35</td>
</tr>
<tr>
<td>Forest Fires in China</td>
<td>Land Area</td>
<td>1.25</td>
</tr>
<tr>
<td>East/West Power Grid</td>
<td>Megawatts</td>
<td>1</td>
</tr>
<tr>
<td>Earthquakes</td>
<td>Energy, Area</td>
<td>1</td>
</tr>
<tr>
<td>Asteroids</td>
<td>Energy</td>
<td>1</td>
</tr>
<tr>
<td>Pacific Hurricanes</td>
<td>Energy</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Asset/Sector</th>
<th>Consequence</th>
<th>Exponent High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hurricanes</td>
<td>$Loss$</td>
<td>0.98</td>
</tr>
<tr>
<td>Public Switched Telephone</td>
<td>Customer-Minutes</td>
<td>0.91</td>
</tr>
<tr>
<td>Forest Fires</td>
<td>Land Area</td>
<td>0.66</td>
</tr>
<tr>
<td>Hurricanes</td>
<td>Deaths</td>
<td>0.58</td>
</tr>
<tr>
<td>Earthquakes</td>
<td>$Loss$</td>
<td>0.41</td>
</tr>
<tr>
<td>Earthquakes</td>
<td>Deaths</td>
<td>0.41</td>
</tr>
<tr>
<td>Wars</td>
<td>Deaths</td>
<td>0.41</td>
</tr>
<tr>
<td>Whooping Cough</td>
<td>Deaths</td>
<td>0.26</td>
</tr>
<tr>
<td>Measles</td>
<td>Deaths</td>
<td>0.26</td>
</tr>
<tr>
<td>Small Fires in Cities</td>
<td>$Loss$</td>
<td>0.07</td>
</tr>
</tbody>
</table>

Low risk hazards: $q \geq 1$

High risk hazards: $q < 1$
Large Floods

- Large floods are high risk (Table 2-9 in Text).

![Graphs showing probability and discharge size relationship]
Natural Disasters

- Natural disasters in the US (Table 2-10 in Text).
Levy Flights

- Levy flights (or Levy walks) are displacements in distance or time between events.
- **Distance**: The distribution of the distance between hazardous events obeys a power law.
- **Time**: The distribution of time elapses between subsequent hazardous events obeys a power law.
- **Or in more simple terms**
  - When the likelihood of a hazard is distributed according to a long-tailed power law, the hazard is said to “take a Levy flight”, which is a series of random, but somewhat related hazards separated in time. Hence, most hazardous events happen in clusters separated by short intervals. A Levy flight in distance is a series of random, but somewhat related hazards separated in space. Hence, most hazardous events occur near one another.

Note: The term Levy flight was coined by Benoît Mandelbrot and named for French mathematician Paul Levy who was known for his work in probability theory.
SARS Levy Flight

- Distance distribution of the spread of SARS (Figure 2-11 in Text).
Al-Qaeda attacks obey Levy flights in terms of **deaths**, time, and distance between incidents (Figure 2-12 in Text).
Al-Qaeda Threats (Cont.)

- Al-Qaeda attacks obey Levy flights in terms of deaths, time, and distance between incidents (Figure 2-12 in Text).
Al-Qaeda Threats (Cont.)

- Al-Qaeda attacks obey Levy flights in terms of deaths, time, and distance between incidents (Figure 2-12 in Text).
Exceedance probability and PML Risk is a better measure of risk in infrastructure systems containing many assets linked together as a network.

- Exceedance $E$ is often a power law
- Fractal dimension, $q$ equals the slope of $E$
- PML risk is a function of consequence, $C$
- PML risk is either low or high, depending on $q$.
  - Low risk: $q \geq 1$
  - High risk: $q < 1$.  

System Risk Summary
Hazards obey Levy flights in time and space if their distributions obey a power law.

- Hazardous events are separated in space and time according to a power law distribution.
- This means they are (partially) predictable as a posteriori probabilities.
- Many hazards are Levy flights in time and space.
  - Terrorism
  - Infectious diseases