A Literature Review and Proposed Method of Measuring a Reduction in Vulnerability at an Airport Checkpoint

Alex Moscoso
TSA Economic Analysis Branch

Presentation for the Society of Benefit-Cost Analysis Conference
March 19, 2015
Regulations & Security

- Executive Orders (EO) 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits.

- EO 12866 requires agencies to determine whether a regulatory action is significant, has an annual effect on the economy of $100 million or more, and therefore subject to review by Office of Management and Budget (OMB).

- EO 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility.

- Office of Management of Budget Circular A-4

- Security rulemaking from DHS, TSA, USCG, CBP.
Layered Security Approach


- “…rationale for using multiple layers is that no security element provides perfect protection, and multiple layers of different types of security...provides protection against the inevitable shortcomings with any individual element.”

- Redundant costs and technologies and diminishing returns.
- Performance depends, not only on inherent performance of individual elements, but on the interactions between elements.
- Possible to have both positive and negative interaction between elements.
Challenges to Quantifying Security Risk

  - “Because the benefits of homeland security regulation are a function of the likelihood and severity of a hypothetical future terrorist attack, they are very difficult to forecast, quantify, and monetize.”

  - Benefits-cost analysis has yet to overcome two analytical challenges estimating baseline risk and effects of proposed measure on risk: (1) lack of historical data and (2) inability to anticipate how terrorists will adapt to changes (Ezell et al., 2010; Merrick and Parnell, 2011; National Research Council, 2010).

  - Argues for “low-resolution” models in policy decisions. However, “high-resolution are quite useful for developing analysts and decisionmakers understanding of risk”.


Defining Security Risk


\[ R(\text{terrorist attacks}) = p(\text{attempted attacks}) \times q(\text{success | attempt}) \times [-u(\text{consequences})] \]


\[ \text{Risk} = f(C,V,T) \]

\[ \text{Risk} = C \times V \times T \]
Quantitative Methods – Willingness to Pay

  - “In monetizing health and safety benefits, the agency should use the WTP measure (or, if appropriate, the WTA measure), rather than other alternatives (e.g., avoided cost of illness or avoided lost earnings). This is because WTP/WTA attempts to capture pain and suffering and other quality-of-life effects.”

  - Stated preference vs Revealed preference method
  - Time consuming, survey based
Quantitative Methods – Break Even

• OMB Circular A-4.
  • “When quantification and monetization are not possible, many agencies have found it both useful and informative to engage in threshold or “breakeven” analysis. This approach answers the question, “How large would the value of the non-quantified benefits have to be for the rule to yield positive net benefits?”

  • Approach focuses on reductions in the number of successful attacks, rather than the potential for the rule to reduce vulnerability or mitigate consequences of an attack.
  • Does not allow for evaluation of reduction in probabilities from multiple types of attacks, focuses on an individual scenario.
  • Doesn’t account for threat response.
  • Doesn’t provide information on efficiency.
Quantitative Methods – Probabilistic Risk Assessment

  • Risk Management Solutions, model for insurance companies used to measure probability and consequences of attack.

  • Article describes a framework for using probabilistic risk modeling to conduct break-even analyses of a regulatory action motivated by terrorism security.
  • Probabilistic risk modeling has two advantages over the individual scenario avoidance approach. First, by incorporating a wide range of potential attack scenarios, the overall risk provides a more comprehensive picture of the terrorist threat that includes both more likely but lower consequence attack scenarios as well as low probability, catastrophic attack scenarios. Second, by including the relative likelihood of many different modes of attacks on many different targets, this approach is capable of reflecting the effect that security can have on changes in terrorists’ preferences for attack and the resulting changes in terrorism risk.
  • Used RMS to with break-even analysis to develop a curve showing comparing the impact in losses to risk reduction needed to break-even
Quantitative Methods – Fault Tree Analysis

- “Fault trees quantify program impact on event likelihood by modeling how programs can act individually and in concert to manage risk.”

* Probabilities in fault tree are arbitrary and do not represent actual airport screening data or insight
Proposed Fault Tree for Airport Checkpoints

* Probabilities in fault tree are arbitrary and do not represent actual airport screening data or insight
Inputs and Risk Register

• Each node in the fault tree would have inputs: \( P(d) \), \( P(n) = 1 - P(d) \).
• Consequences would have inputs of probability (threat) and impact.
• Other inputs could include: synergistic relationship, etc.
• Sources: Lab test, field data, and experts’ subjective judgment.

<table>
<thead>
<tr>
<th>Countermeasures</th>
<th>Probability of Detection</th>
<th>Likelihood of Occurrence</th>
<th>Impact ($ millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Med</td>
<td>High</td>
</tr>
<tr>
<td>Police-Dog Units</td>
<td>0.5</td>
<td>0.75</td>
<td>0.9</td>
</tr>
<tr>
<td>Checked Baggage X-Rays</td>
<td>0.3</td>
<td>0.6</td>
<td>0.75</td>
</tr>
<tr>
<td>Behavior Detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID Verification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carry-On Baggage X-Ray</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passenger Screening</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pat Down Screening</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consequences</th>
<th>Likelihood of Occurrence</th>
<th>Impact ($ millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Med</td>
</tr>
<tr>
<td>Non-metallic body bomb</td>
<td>0.000001</td>
<td>0.0003</td>
</tr>
<tr>
<td>Carry-on bomb</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Armed Assualt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Values in the risk register are arbitrary and do not represent actual airport screening data or insight
Concerns with Subjective Judgment

  - Judgments are necessarily used in the study of complex technical problems, essential to analysis
  - Quantification does not mean certainty, indicate best guess and uncertainty. Capturing uncertainty is critical

- Kousky. 2011.
  - Costly and time sensitive
  - False sense of precision
Dealing with Uncertainty

• Innate uncertainty in expert judgments, and even lab and field data, calls for statistical remedy.
• Monte Carlo Simulation preferred to High/Low
  • Quickly calculates likelihoods for multiple outcomes in complex systems with multiple varying factors (fault tree) through tens of thousands of iterations
  • Narrows the distributions of possible outcomes
Different Types of Attacker

• Inputs should alter with the type of attackers:

  • Savvy Attacker
    • Attacker has planned for a long time, reconnaissance
    • Attacker is well-trained
    • Affiliated with group, has support

  • Non-savvy Attacker
    • Little to no planning
    • Little to no training
    • Self-radicalized
Calculating Overall Risk

- Weighted average for portfolio of scenarios
  - Threat = Likelihood to occur from intelligence reports
  - Consequences = Comprehensive cost analysis
  - Vulnerability = Fault tree analysis

<table>
<thead>
<tr>
<th>Attack Scenarios</th>
<th>Threat Likelihood of Occurrence</th>
<th>Vulnerability Security Effectiveness</th>
<th>Risk-Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Scenario 1 w/ Savvy Attacker</td>
<td>0.2</td>
<td>0.12</td>
<td>0.024</td>
</tr>
<tr>
<td>Attack Scenario 1 w/ Non-savvy Attacker</td>
<td>0.1</td>
<td>0.09</td>
<td>0.009</td>
</tr>
<tr>
<td>Attack Scenario 2</td>
<td>0.4</td>
<td>0.33</td>
<td>0.132</td>
</tr>
<tr>
<td>Attack Scenario 3 - w/ Savvy Attacker</td>
<td>0.1</td>
<td>0.19</td>
<td>0.019</td>
</tr>
<tr>
<td>Attack Scenario 3 - w/ Non-savvy Attacker</td>
<td>0.2</td>
<td>0.13</td>
<td>0.026</td>
</tr>
<tr>
<td><strong>Total Risk Profile</strong></td>
<td></td>
<td></td>
<td><strong>0.21</strong></td>
</tr>
</tbody>
</table>

*Values in the table are arbitrary and do not represent actual airport screening data or insight.*
Measuring Change in Vulnerability and Risk

- Change in vulnerability is the difference between vulnerability in the baseline ($V^b$) and vulnerability with added layer ($V^a$)
  - Sum all the likelihoods of threat making it through layered system = Vulnerability
- Run fault tree for all applicable scenarios
  - Run Monte Carlo to incorporate range of uncertainty for certain inputs
- Functional form for change in risk:

$$\Delta R = \sum_{i=1}^{m} R^b_i - \sum_{i=1}^{m} \sum_{j=1}^{n} R^a_{ij} = \sum_{i=1}^{m} T_i V^b_i C_i - \sum_{i=1}^{m} \sum_{j=1}^{n} T_i V^a_{ij} C_i$$

$i=1,2,..., m$: number of attack scenarios;
$j=1,2,..., n$: number of security layers
$b$: baseline, $a$: added security layer
Questions?