Prioritizing Terrorism Vulnerability Analyses for Critical Infrastructure Sectors

Don N. Kleinmuntz

Strata Decision Technology

Henry Willis

Rand Corporation

Decision Analysis Affinity Group Meeting

Indianapolis, IN

May 18, 2009

Acknowledgements & Disclaimers

- Supported by United States Department of Homeland Security (US-DHS) through grant to National Center for Risk and Economic Analysis of Terrorism Events (CREATE)
- Based on problem and data provided by California Governor’s Office of Homeland Security (CA-OHS)

- Data included sensitive (but not secret) information, and both data and other details have been modified to disguise sensitive information
- *Any opinions, findings, conclusions, or recommendations are those of the presenter and do not necessarily reflect views of US-DHS or CA-OHS*

USC CREATE HOMELAND SECURITY CENTER

Vulnerability Assessments of State's Critical Infrastructure Sectors

- Critical infrastructure vulnerability assessments
  - Crucial in allocation of counterterrorism resources – which are the most vulnerable sites?
  - Essential first step in development of protection plans
- Performed by California's CIP-FSIVA team
  - *Critical Infrastructure Protection – Full Spectrum Infrastructure Vulnerability Assessment*
  - State national guard program in support of state/local agencies, private sector, Department of Defense
  - Inspections performed by invitation only, in cooperation with state/local authorities

Challenges in Prioritizing Sectors

- Which sectors should be analyzed first?
  - Inspection/analysis is time consuming and capacity is limited
  - More efficient if done one sector at a time
  - Multi-year effort to work through sectors
- Data difficult to get, difficult to use, difficult to analyze
  - Hundreds of critical sites, close to 30 sectors being considered
  - Site- or sector-specific threat probabilities are difficult to assess
  - Information is incomplete and incomparable across sectors
  - Economic consequences are large but difficult to assess with precision
  - Risk management plans do not exist or are incomplete
- Need approach for using *high-level* expert assessments to select sectors for further study and analysis
  - Recognize that inputs to the model will be vague
  - Recognize that time and resources available to support the selection of sectors are limited

The Approach

1. Identify Sectors
   - Identify number of critical sites in each sector
2. Elicit Expert Risk Assessments
   - Protocol allows for vague/imprecise assessments
   - Threat, vulnerability, & consequences for each sector
3. Analyze Value of Vulnerability Analyses
   - Use risk analysis to estimate benefit of performing vulnerability analyses on the critical sites in each sector
4. Allocate Limited Analysis Capability to Sectors
   - Identify sectors that provide most benefit from limited capacity
5. Perform Vulnerability Analyses

Step 1: Identify Sectors

- Broad categories of interest
  - Agriculture & Food
  - Banking & Finance
  - Commercial Facilities
  - Energy Sector
  - Government Facilities
  - Information Technology & Telecommunication
- Broken into smaller sectors of specific types
  - 29 sectors and 702 sites
  - Sites per sector ranged from 1 to over 300 each
  - Assumed that would be able to prescreen to 25 most critical sites

Sector Prioritization Pilot Study

- Goal: Develop and test methods for prioritizing which infrastructure sectors FSIVA should analyze
- Assessments and relevant data provided by:
  - Governor's Office of Homeland Security
  - U.S. DHS Protective Security Advisor Program (PSA's)
  - State sector subject matter experts
  - State Terrorism Threat Assessment Center (STTAC)
  - Regional Terrorism Threat Assessment Centers (RTTACs)

Step 2: Elicit Expert Risk Assessments

- Use expert elicitation panel to obtain assessments
  - Governor’s Office of Homeland Security
  - U.S. DHS Protective Security Advisor Program (PSA’s)
  - State sector subject matter experts
  - State Terrorism Threat Assessment Center (STTAC)
  - Regional Terrorism Threat Assessment Centers (RTTACs)
- Protocol allows for vague/imprecise assessments
  - Threat: Rank order threat of attack on each sector
  - Other inputs: Elicit ranges (lower and upper bounds)
  - Define anchored scales to support range assessment

Assessments: Threat

- Threat = Probability of attack
  - Suppose you know an attack would take place in California next year, but the target is unknown
  - Rate the relative likelihood the attacker would select one or more critical sites in each sector
- Use rating scale from 0 to 10
  - 0 means "possible but extremely unlikely"
  - 5 means "moderately likely"
  - 10 means "extremely likely"
- Note that this is an *ordinal* scale
  - Translation from ranks into probabilities is problematic

Assessment: Vulnerability

- Vulnerability = Probability attack would succeed if attempted
  - Suppose an attack occurred against a particular site in each sector
  - Rate the probability that the attack would succeed in causing significant damage, including loss of life and direct or indirect economic losses
  - **Provide both a lower and upper bound**.
- Use 0 to 10 rating scale, defined as follows:
  - 10 Probability of terrorist success greater than 95%
  - 9 Probability of terrorist success from 85% and 95%
  - 8 Probability of terrorist success from 75% and 85%
  - and so on, down to...
  - 1 Probability of terrorist success from 5% and 15%
  - 0 Probability of terrorist success less than 5%

Assessments: Consequences

Fatalities

- If a successful attack were to occur against a particular site in this sector, what is the range of expected fatalities?
- **Provide both a lower and upper bound.**
- Use a 0 to 7 rating scale:
  - 7 More than 1 million
  - 6 From 100,000 to 1 million
  - 5 From 10,000 to 100,000
  - 4 From 1,000 to 10,000
  - 3 From 100 to 1,000
  - 2 From 10 to 100
  - 1 From 1 to 10
  - 0 None
- *Computed monetary-equivalent loss using value of $6 million per fatality*

Economic Loss

- If a successful attack were to occur against a particular site in this sector, what is the range of expected direct economic losses (damage to property and interruption of functioning of public and private institutions)?
- **Provide both a lower and upper bound.**
- Use a 0 to 7 rating scale:
  - 7 More than $1 trillion
  - 6 From $100 billion to $1 trillion
  - 5 From $10 billion to $100 billion
  - 4 From $1 billion to $10 billion
  - 3 From $100 million to $1 billion
  - 2 From $10 million to $100 million
  - 1 From $1 million to $10 million
  - 0 Less than $1 million

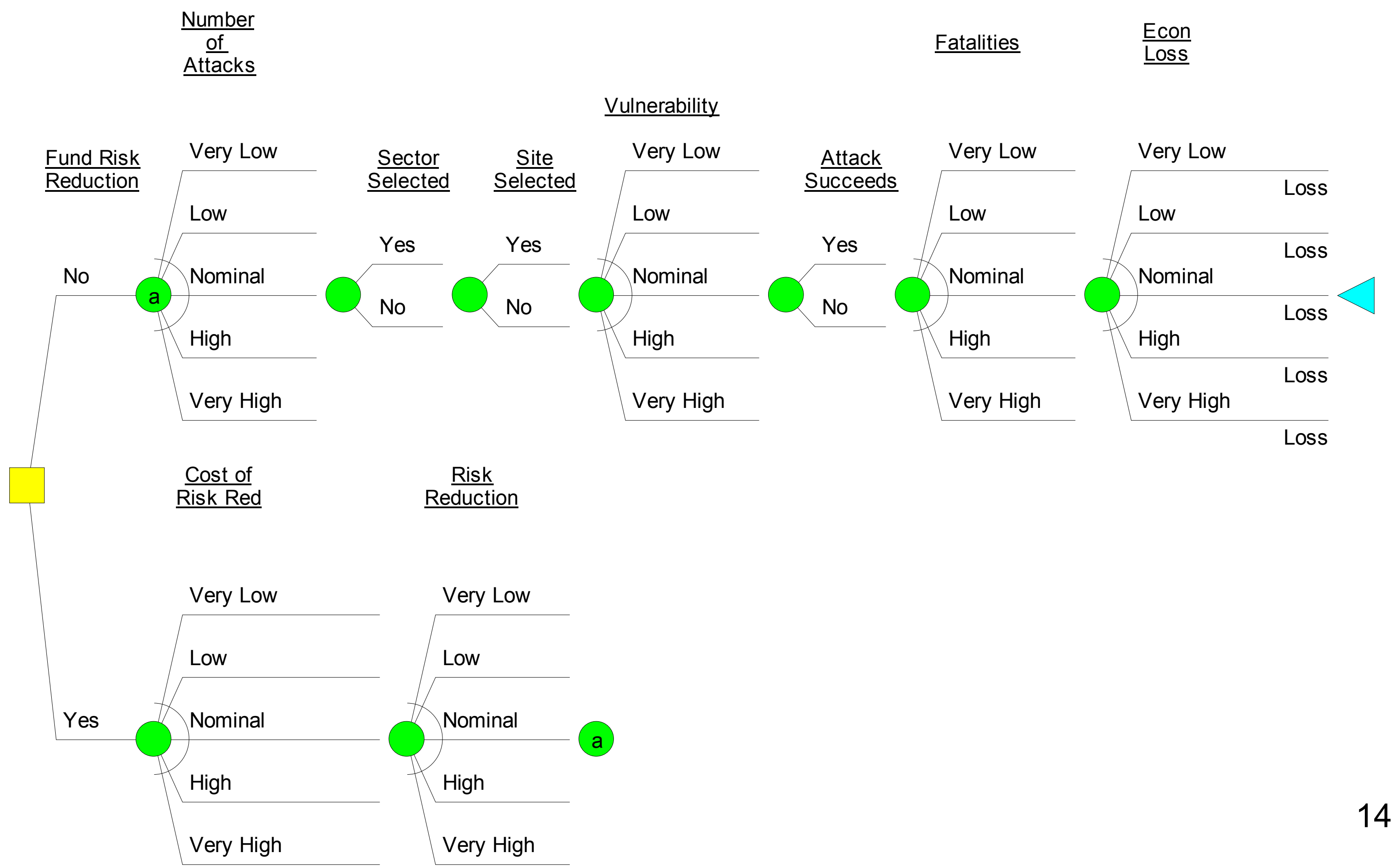
	Sites	Threat	Vulnerability		Fatalities		Econ. Loss	
ID	N	T	VL	VU	FL	FU	EL	EU
1	14	0.0655	0%	35%	10	100,000	1	1,000
2	7	0.0655	0%	45%	10	10,000	0	10,000
3	25	0.0573	5%	25%	1	10,000	1	100
4	1	0.0573	25%	95%	1	10,000	0	100,000
5	18	0.0492	0%	45%	0	100	1	10,000
6	1	0.0492	0%	25%	1	100	0	10
7	2	0.0492	0%	5%	1	1,000	1	1,000
8	7	0.0492	0%	35%	10	10,000	0	100
9	3	0.0492	0%	15%	10	10,000	0	10,000
10	3	0.0410	0%	95%	0	100	1	100,000
11	2	0.0410	0%	65%	0	100	1	100,000
12	25	0.0410	0%	25%	0	1,000	1	100,000
13	1	0.0410	0%	45%	1	10,000	1	10,000
14	15	0.0410	55%	75%	1	100	0	10
15	11	0.0410	0%	100%	0	1,000	0	100,000
16	2	0.0410	0%	25%	0	1,000	10	100,000
17	3	0.0410	0%	100%	0	1,000	1	100,000
18	6	0.0410	5%	25%	1	1,000	1	1,000
19	25	0.0328	45%	75%	100	1,000,000	10	1,000
20	21	0.0328	45%	75%	100	1,000,000	10	1,000
21	24	0.0246	75%	95%	100	1,000,000	1	100
22	25	0.0164	55%	75%	100	10,000	10	1,000
23	25	0.0164	0%	45%	1	100	0	100
24	2	0.0082	65%	95%	100	10,000	10	10,000
25	23	0.0082	5%	25%	0	1,000	10	100,000
26	25	0.0001	45%	85%	1	100	0	10
27	6	0.0001	0%	75%	0	1,000	0	1,000
28	3	0.0001	0%	65%	0	1,000	10	100,000
29	2	0.0001	0%	65%	0	100	0	10,000

Assessment Required Several Hours

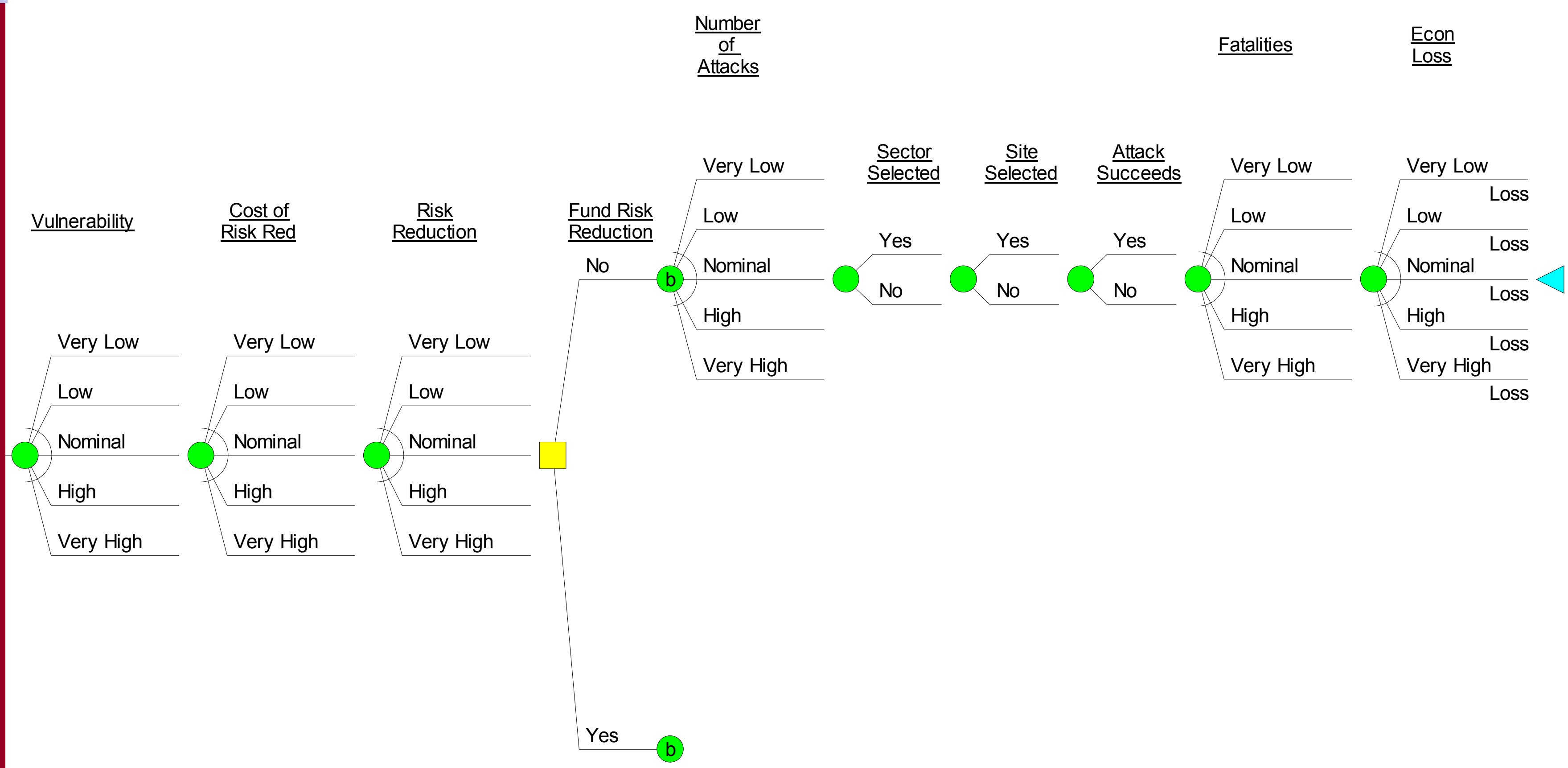
Step 3: Value of Vulnerability Analyses

- Suppose OHS selects a particular sector for vulnerability analyses of critical sites
  - How much reduction in expected losses could potentially be achieved for each site?
  - How much incremental reduction is possible with from performing risk reduction?
- Approach:
  - Initial analysis is a classic Expected Value of Perfect Information (EVPI) formulation
  - EVPI is an **<u>upper bound</u>** for value of vulnerability analyses
    - Assumes that vulnerability analyses resolve some uncertain ranges to a point estimate (hence the label <u>perfect</u> information)

Choice Problem
Without Vulnerability Analysis



Choice Problem with Vulnerability Analysis (Perfect Info.)



Value of Vulnerability Analyses: Technical Assumptions

- Decompose P(Attack) into three components:
  1. Number of attacks attempted against sites in California:
     Poisson distribution, mean = avg. no. of attacks per 10 years (e.g., 2/decade)
  2. Probability of an attack being against this sector:
     Threat ranking, translated into a probability
  3. Probability that this site is selected:
     Each site equally likely (1/N)
- Vulnerability: Uniformly distributed across assessed range
- Consequences: Uniformly distributed across assessed ranges
- Risk Reduction: Risk reduction plan reduces expect loss by percentage uniformly distributed across range [0% to 30%]
- Cost: Cost for each risk reduction plan uniformly distributed across range [$1M to $5M]
- Value of Vulnerability Analysis =
  Expected losses without analysis – Expected losses with analysis

Results:
EVPI per Site

- Expected losses from $0 to $6 billion
- EVPI much lower
  - $0 to $1.1 million
- Risk reduction can lower expected loss substantially even without prior information
  - Would OHS *ever* recommend risk reduction without vulnerability analysis?

EV(No RR)	EV(RR)	EV(VA)	EVPI
492.119	421.301	421.245	0.056
147.501	128.376	128.122	0.254
41.330	38.130	37.545	0.585
5501.006	4676.155	4676.155	0.000
6.520	8.542	6.460	0.059
3.788	6.220	3.782	0.006
4.309	6.663	4.299	0.011
73.997	65.897	65.418	0.480
86.174	76.248	75.818	0.430
653.038	558.108	558.074	0.034
670.254	572.716	572.683	0.033
21.730	21.471	20.366	1.104
645.815	551.942	551.908	0.034
1.094	3.930	1.094	0.000
197.545	170.914	170.732	0.181
271.650	233.903	233.780	0.123
724.340	618.689	618.660	0.029
7.182	9.105	7.127	0.055
4724.467	4108.797	4108.797	0.000
5624.366	4783.711	4783.711	0.000
5228.111	4446.894	4446.894	0.000
28.291	27.048	26.445	0.603
0.104	3.089	0.104	0.000
231.601	199.861	199.814	0.047
5.669	7.819	5.648	0.022
0.002	3.001	0.002	0.000
0.044	3.037	0.044	0.000
1.148	3.976	1.148	0.000
0.172	3.146	0.172	0.000

Results:
EVPI per Site

- Expected losses from $0 to $6 billion
- EVPI much lower
  - $0 to $1.1 million
- Risk reduction can lower expected loss substantially even without prior information
  - Would OHS *ever* recommend risk reduction without vulnerability analysis?

EV(No RR)	EV(VA)	EV of VA
492.119	421.245	70.874
147.501	128.122	19.379
41.330	37.545	3.784
5501.006	4676.155	824.851
6.520	6.460	0.059
3.788	3.782	0.006
4.309	4.299	0.011
73.997	65.418	8.579
86.174	75.818	10.356
653.038	558.074	94.964
670.254	572.683	97.571
21.730	20.366	1.364
645.815	551.908	93.906
1.094	1.094	0.000
197.545	170.732	26.813
271.650	233.780	37.870
724.340	618.660	105.680
7.182	7.127	0.055
4724.467	4108.797	615.670
5624.366	4783.711	840.655
5228.111	4446.894	781.217
28.291	26.445	1.846
0.104	0.104	0.000
231.601	199.814	31.787
5.669	5.648	0.022
0.002	0.002	0.000
0.044	0.044	0.000
1.148	1.148	0.000
0.172	0.172	0.000

USC

CREATE HOMELAND SECURITY CENTER

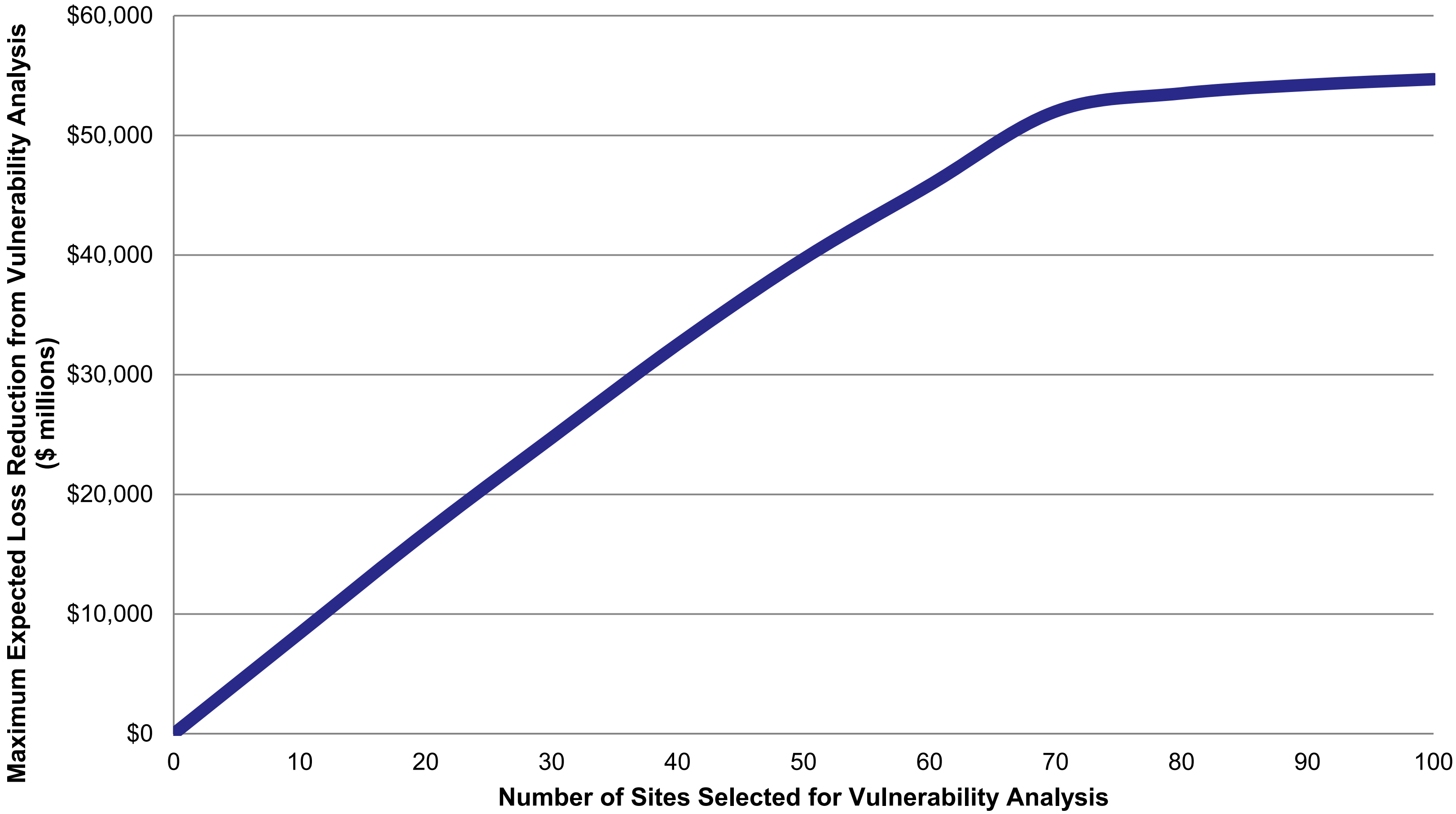
Step 4: Prioritize Sites & Sectors

- Portfolio allocation problem
  - Choose best set of sites and sectors
- Objective: Maximizing aggregate expected reduction of losses
- Subject to constraints:
  - Maximum number of sites that FSIVA can analyze in available time
  - May choose anywhere from 0 to N_i sites, where N_i is number of critical sites in sector i
- This is an integer linear programming problem

	Optimization	
EV of VA	Sites Chosen	Loss Reduction
70.874	14	992.230
19.379	0	0.000
3.784	0	0.000
824.851	1	824.851
0.059	0	0.000
0.006	0	0.000
0.011	0	0.000
8.579	0	0.000
10.356	0	0.000
94.964	3	284.892
97.571	2	195.142
1.364	0	0.000
93.906	1	93.906
0.000	0	0.000
26.813	2	53.626
37.870	2	75.740
105.680	3	317.041
0.055	0	0.000
615.670	25	15391.753
840.655	21	17653.753
781.217	24	18749.199
1.846	0	0.000
0.000	0	0.000
31.787	2	63.574
0.022	0	0.000
0.000	0	0.000
0.000	0	0.000
0.000	0	0.000
0.000	0	0.000
	100	54695.708
constraint:	100	MAX

	Constraint:										
Sector	0	10	20	30	40	50	60	70	80	90	100
1	0	0	0	0	0	0	0	0	0	10	14
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	1	1	1	1	1	1	1	1
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	3	3	3
11	0	0	0	0	0	0	0	0	2	2	2
12	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	1	1	1
14	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	2
16	0	0	0	0	0	0	0	0	0	0	2
17	0	0	0	0	0	0	0	0	3	3	3
18	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	4	14	24	25	25	25
20	0	10	20	21	21	21	21	21	21	21	21
21	0	0	0	8	18	24	24	24	24	24	24
22	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	2
25	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0
Value:	0	8407	16813	24728	32541	39690	45847	52004	53511	54219	54696

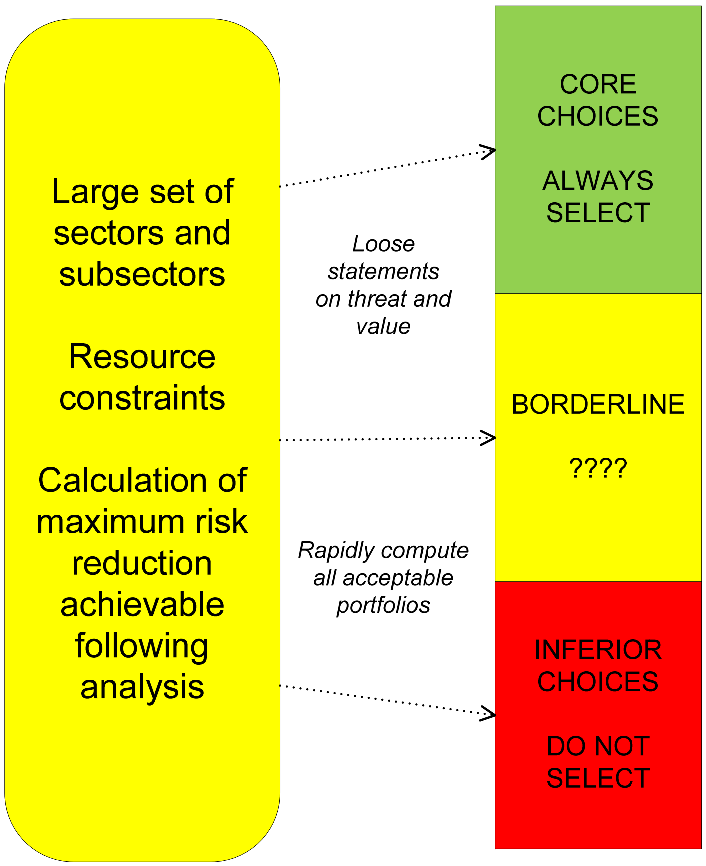
Maximum Value of Vulnerability Analysis versus Number of Sites Analyzed



Discussion and Implications

- Value measure is an upper bound
  - Assumes no current knowledge to differentiate specific sites within sectors
  - Assumes vulnerability analyses will produce definitive results
  - Does not consider strategies to “carve out” specific sites within sectors (e.g., analyze only a select subset of a sector)
- Assumes that cost and time required for vulnerability analyses do not vary by sector or by site within sector
- Indirect economic consequences not included
- Other critical criteria may also be relevant (e.g., symbolic value, national security impact)
- Results are sensitive to precise translation of ordinal threat ratings into probabilities
  - Robust portfolio methods can handle this easily (coming soon!)

Risk-Based Robust Portfolio Modeling



- Embraces inexact assessments like rank orders or imprecise ranges
- Identifies sets of selected sectors that are clearly inferior, and eliminates them
- Method identifies many acceptable portfolios (sets of non-eliminated sectors)
- Looking across portfolios, sectors fall into three groups:
  - **Green: Always selected**
  - **Yellow: Sometimes selected, sometimes not**
  - **Red: Never selected**

USC CREATE HOMELAND SECURITY CENTER

Risk-Based Robust Portfolio Modeling: Refining Results